UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

----------X

ANDREW HILLMAN, MARISSA DEAN, DAWN HARBIN; STEPHANIE OWENS; RYAN GROENEWEG, BILLY GUERINGER; MAULIK PARIKH, RICHARD WEINER; STEVE WILLIAMS; G.G., a minor, by and through parent RHONDA GUERINGER, and J.N., a minor by and through parent SEMYON NAROSOV, individually, on behalf of themselves and others similarly situated,

Plaintiffs,

v.

RINGLEADER DIGITAL, INC., a Delaware Corporation; ACCUWEATHER, INC., a Pennsylvania Corporation; CABLE NEWS NETWORK, a Delaware Corporation; ESPN, INC., a Delaware Corporation; FOX NEWS NETWORK, LLC, a Delaware Corporation; GO2 MEDIA, INC., a Delaware Corporation, MERRIAM-WEBSTER, INC., a Delaware Corporation; TRAVEL CHANNEL, LLC, a Delaware Corporation; and WHITEPAGES, INC., a Delaware Corporation;

Defendants.

----------X

10 CV 8315

Civil Action No _____

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

Plaintiffs, on behalf of themselves and all other similarly situated individuals (collectively, "Plaintiffs," each a "Class Member" of the putative "Class" as further defined herein), by and through their attorneys, KamberLaw, LLC, and the Law Offices of Joseph H. Malley, P.C., as and for their complaint and demanding trial by jury, allege as follows based on their personal knowledge as to themselves and their own acts and observations and, otherwise,

upon information and belief based on the investigation of counsel, which Plaintiffs believe further investigation and discovery will support with substantial evidence.

NATURE OF THE ACTION

1. Plaintiffs bring this consumer class action lawsuit pursuant to Federal Rules of Civil Procedure 23(a), (b)(1), (b)(2), and (b)(3) on behalf of themselves and a class of similarly situated individual Internet users who were victims of privacy violations and unfair business practices; wherein their privacy, financial interests, and security rights, were violated by the following Defendants: Ringleader Digital, Inc., (hereinafter referred to as "Ringleader"), AccuWeather, Inc., (hereinafter referred to as "AccuWeather"), Cable News Network, Inc., (hereinafter referred to as "CNN"), ESPN, Inc., (hereinafter referred to as "ESPN"), FOX News Network, LLC, (hereinafter referred to as "FOX"), Go2 Media, Inc., (hereinafter referred to as "Go2 Media"), Merriam-Webster, Inc., (hereinafter referred to as "Merriam-Webster"), Travel Channel, LLC, (hereinafter referred to as "Travel Channel"), and WhitePages, Inc., (hereinafter referred to as "WhitePages"), affiliated individually and in concert with Ringleader, referred collectively to as, "Ringleader Digital Affiliates," to gain unauthorized access to, and unauthorized use of, Plaintiffs and Class Members' mobile devices referencing electronic devices used for communication over a cellular network and include internet and multimedia capabilities, which include but are not limited to: iPhone, iPad, iTouch and Personal Digital Assistants ("PDA's"), with HTML5 client side storage capability; hereinafter referred to collectively as "mobile devices."

2. Defendants gained unauthorized access to, and unauthorized use of, Plaintiffs and Class Members' mobile telephone devices, bypassing the technical and code-based barriers intended to limit access, in addition to bypassing the Plaintiffs and Class Members' privacy and

security settings. Defendants perpetuated this to individually identify Plaintiffs and monitor their web-browsing activities on their mobile phones.

3. Ringleader acted independently, and in concert individually with the Ringleader Digital Affiliates, and each knowingly authorized, directed, ratified, approved, acquiesced in, or participated in conduct, made the basis of this Class action, which included, but was not limited to, the unauthorized access to, and unauthorized use of the Plaintiffs and Class Members' mobile devices.

4. Defendants' purpose was to conduct mobile tracking of Ringleader Digital Affiliate users which would allow access to, and disclosure of, Personal Information ("PI"), Personal Identifying Information ("PII"), and/or Sensitive identifying information ("SII") derived from the user's mobile device, and linked to the user's device, involving activities, including but not limited to, users' activities on Ringleader Digital Affiliates' websites, which Defendants accomplished covertly, without actual notice, awareness, consent or choice of its users, and

5. Essentially, Defendants hacked the mobile phones of millions of consumers' mobile phones by embedding a tracking code in each user's mobile device database to circumvent users' browser controls for managing web privacy and security which information Defendants obtained deceptively, for purposes not disclosed within their Terms of Service and/or Privacy Policy, obtained for Defendant's commercial gain.

6. The sequence of events related to this action include, but are not limited to the following:

a) Plaintiffs and Class Members are individuals in the United States who own mobile devices and use their mobile devices to access websites on the Internet and visited one of

the Ringleader Digital Affiliate's websites within the class period. Plaintiff and Class Member J.N., a minor, age twelve (12) years old, is a minor under, the age of thirteen (13) that visited one of the Ringleader Digital Affiliates websites within the class period and did not obtain protection from the Defendant's act as protected by COPPA, The Children's Online Privacy Protection Act of 1998 (COPPA), a United States federal law, located at 15 U.S.C. § 6501–6506 (Pub.L. 105-277, 112 Stat. 2581-728, enacted October 21, 1998).

b) Plaintiffs and Class Members visited the websites of the Defendant Ringleader Digital Affiliates within the class period and then Defendant Ringleader, acting in concert individually with Ringleader Digital Affiliates, gained unauthorized access to, and unauthorized use of, the Plaintiffs and Class Members mobile device, without their notice or consent.

c) Defendant(s) then transmitted a program, information, code, and/or command within the Plaintiffs and Class Members' mobile device to scan, copy and use without notice, consent, or authority, the Plaintiffs and Class Members mobile device, obtaining mobile device configuration, a practice not necessary for the placement of persistent cookies for tracking website visitors, nor an acceptable practice within the industry. While traditional advertisers access the users' browser for online tracking, Defendants access involved areas of the Plaintiffs and Class Members' mobile devices(s) that involved hardware and software associated with non-browser activity.

d) Defendant Ringleader then created, without notice, consent, or authority, a database for use by Defendant Ringleader within the Plaintiffs and Class Members mobile device which did not previously exist, nor was designed by the manufacturers of the mobile device for the use intended by Defendants.

e) Defendant Ringleader then created, in concert individually with Defendant Ringleader Digital Affiliates, a database for use by Defendant Ringleader Digital Affiliates, without notice, consent, or authority, an additional unauthorized database on the Plaintiffs and Class Members mobile device, then downloaded additional tracking code to assist the Defendant Ringleader's tracking scheme. Such tracking codes could not easily be detected, managed or deleted, and provided, in whole or part, the collective mechanism to track Plaintiffs and Class Members, without notice, consent, or authority.

f) Defendant(s) then configured a Unique Device Identifier ("UDID") derived in whole or part, from the Plaintiffs and Class Members' mobile device properties and "stamped" the UDID within the Plaintiffs and Class Members' mobile device, and stored additional data, to provide a mechanism to back up the mobile device's Identifier for purposes of restoring it later if deleted by the user.

g) Defendant Ringleader then used the Unique Device Identifier within the user's database, to re-spawn the user's Unique Device Identifiers ("UDID's") if deleted by the user, by use, in whole or part, using additional mobile device functions, bypassing Plaintiffs and Class Members privacy and security settings, denying choice and protection if they cleaned their cache, bookmarks, and history.

h) Defendant Ringleader then conducted systematic and continuous surveillance of the Plaintiffs and Class Members' mobile devices, by use of its Unique Device Identifiers ("UDID's") embedded in the user's mobile device, as Plaintiffs and Class Members used their mobile device for additional mobile browsing.

i) Defendants then copied and used the mobile device data within the Plaintiffs and Class Members' mobile devices, after it knowingly accessed, without authorization the Plaintiffs

and Class Members' mobile device. Defendants objective was to copy and use the Plaintiffs and Class Members' mobile device configuration data, alter or delete previous data, if needed, although such data now was present in property owned by Plaintiffs and Class Members although provided by Defendants.

j) Defendants then obtained Plaintiffs and Class Members' personal information, derived, in whole or part, from its monitoring the mobile browsing activities of Plaintiffs and Class Members or specific sites. The personal information Defendants misappropriated and compiled, with information provided from Ringleader and Ringleader Digital Affiliates includes details about user profiles to identify individual users and track them on an ongoing basis, across numerous websites, and tracking users when they accessed the web from different mobile devices, at home and at work. This sensitive information may include such things as users' video viewing choices and personal characteristics such as gender, age, race, number of children, education level, geographic location, and household income, what the web user looked at and what he/she bought, the materials he/she read, details about his/her financial situation, his/her sexual preference, his/her name, home address, e-mail address and telephone number, and even more specific information like health conditions.

k) Defendants then intercepted the Electronic Communications sent to the Plaintiffs and Class Members mobile device, including but not limited to, the Plaintiffs and Class Members' carrier transactional information which included, but not limited to, "carrier network IP," information sought to link location with the Plaintiffs and Class Members since such persisted across Internet sessions. This provided in whole, or in part, what amounted to a "Trap and Trace" of the user's mobile device's functions.

> *"Utilizing the advances in GPS technology, marketers can now determine the precise location of mobile users—within three feet."*

"Acuity Mobile Partners with AlphaTrek to Provide Advanced Location Targeting for Mobile Marketing Clients; Expands Patent Portfolio," 22 Apr. 2008, online: http://www.acuitymobile.com/docs/Press04222008.php (last accessed October 2010)

"The whole focus has been on layering GPS in virtually any type of content, and taking that location awareness down to the content level," Bob Walczak, Ringleader Digital's founder and CEO, said during a panel. The company's ad servers act like decision engines, figuring out when and what advertising messages to send to individuals based on ad category, time of day, the user's GPS-derived location and search query keywords they may have entered.

l) Defendant Ringleader Digital Affiliates did not provide Plaintiffs and Class Members information within its privacy policies concerning its affiliation with Defendant Ringleader, information related to the extent of its tracking, made the basis of this action, nor adequate opt-out information, resulting in the following:

1) Plaintiffs and Class Members that desired to cease tracking by Defendant Ringleader and Ringleader Digital Affiliates by deleting the Defendants' database, had Ringleader continue to track their activities.

2) Plaintiffs and Class Members that became aware of Defendant Ringleader's association with the Ringleader Digital Affiliates, were unable to delete the Ringleader database from within their mobile device to cease all tracking. Those that located the Ringleader's website were advised, "Do not just delete cookies or the database in your device."

m) Plaintiffs and Class Members involved with the Defendants were harmed by its practices including but not limited to, incurred time and costs to repair their mobile device, damage to their mobile devices, and limitation to functionality of their mobile devices.

7. Defendants then used third party analytics software to process any and all data derived from all sources, acts that also violates the Plaintiffs and Class Members' mobile device manufacturer's agreement:

"3.3.9 You and Your Applications may not collect, use, or disclose to any third party, user or device data without prior user consent, and then only under the following conditions:

- The collection, use or disclosure is necessary in order to provide a service or function that is directly relevant to the use of the Application. For example, without Apple's prior written consent, You may not use third party analytics software in Your Application to collect and send device data to a third party for aggregation, processing, or analysis.

- The collection, use or disclosure is for the purpose of serving advertising to Your Application; is provided to an independent advertising service provider whose primary business is serving mobile ads (for example, an advertising service provider owned by or affiliated with a developer or distributor of mobile devices, mobile operating systems or development environments other than Apple would not qualify as independent); and the disclosure is limited to UDID, user location data, and other data specifically designated by Apple as available for advertising purposes."

8. Plaintiffs and Class Members that became aware that Defendant Ringleader had created a database, and deleted the databases to cease any and all tracking, had the tracking device re-spawn. The failure of Defendants to provide the user notice of its tracking mechanism within their mobile devices allowed a perpetual re-spawning, creating in effect: "Zombie Databases."

JURISDICTION AND VENUE

9. Venue is proper in this District under 28 U.S.C. §1391(b) and (c) against Defendants. A substantial portion of the events and conduct giving rise to the violations of law complained of herein occurred in this District and Defendants conducts business with consumers in this District. Defendant Ringleader's principle executive offices and headquarters are located in this District at 286 Fifth Avenue, 6th Floor, New York, NY 10001.

10. Subject-matter jurisdiction exists in this Court related to this action pursuant to 28 U.S.C. § 1332. The aggregate claims of Plaintiffs and the proposed Class Members exceed the sum or value of $5,000,000.00.

11. Venue is proper in this district and vests jurisdiction in the New York state and federal courts in the district of the location of their principal corporate place of businesses. Thus, mandatory jurisdiction in this U.S. District Court vests for any Class Member, wherever they reside, for the mobile device activity made the basis of this action which occurred within the United States. The application of the law of the State of New York should be applied to any mobile device activity made the basis of this action anywhere, within the United States, as if any and all activity occurred entirely in New York and to New York resident. Thus, citizens and residents of all states are, for all purposes related to this instant Complaint, similarly situated with respect to their rights and claims as New York residents, and therefore are appropriately included as members of the Class, regardless of their residency, or wherever the mobile device activity occurred made the basis of this action.

12. The following corporations are Delaware corporations headquartered in New York. Plaintiffs assert claims on behalf of a proposed class whose members are scattered throughout the fifty states and the U.S. territories; there is minimal diversity of citizenship

between proposed Class Members and the Defendants. The aggregate of these claims exceed the sum or value of $5,000,000:

a. Ringleader

b. FOX

13. This Court has personal jurisdiction over the Defendants listed in this paragraph because each of the listed defendants maintains its corporate headquarters in, and the acts alleged herein were committed in New York.

14. The following corporations are citizens of states other than New York, however each of the acts upon which liability is alleged herein were committed by the corporations listed in this paragraph in the state of New York:

a. AccuWeather

b. CNN

c. ESPN

d. Go2 Media

e. Merriam-Webster

f. Travel Channel

g. WhitePages

15. Minimal diversity of citizenship exists in this action, providing jurisdiction as proper in the Court, since Defendant is a corporation headquartered in this District, and Plaintiffs include citizens and residents of this District, and assert claims on behalf of a proposed Class whose members are scattered throughout the fifty states and the U.S. territories; thus there is minimal diversity of citizenship between proposed Class Members and the Defendant.

16. This is the judicial district wherein the basis of the conduct complained of herein involving the Defendants was devised, developed, implemented. The actual interaction of information and data was activated from, and transmitted to and from this District; therefore all evidence of conduct as alleged in this complaint is located in this judicial district.

PARTIES

17. Plaintiff Andrew Hillman ("Hillman"), is a citizen and resident of Dallas, Texas, (Dallas County). On information and belief, Hillman incorporates all allegations within this complaint. At all relevant times herein, Hillman owned a mobile device, used that mobile device, on one or more occasions during the class period, in the city of residence, to access the internet sites of one (1) or more Defendant Ringleader Digital Affiliates' website(s), as noted in section a below, which resulted in Defendants gaining unauthorized access to, and unauthorized use of, Hillman's mobile device, by Defendants as noted in section b below:

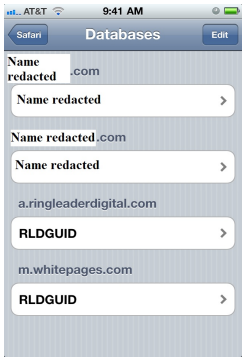
a. www.accuweather.com, a domain name owned by Defendant AccuWeather, Inc., and registered to: AccuWeather, Inc., 385 Science Park Road, State College, PA 16803.

b. 

18. Plaintiff Marissa Dean ("Dean"), is a citizen and resident of Waco, Texas, (McLennan County). On information and belief, Dean incorporates all allegations within this complaint. At all relevant times herein, Dean owned a mobile device, used that mobile device, on

one or more occasions during the class period, in the city of residence, to access the internet sites of one (1) or more Defendant Ringleader Digital Affiliates' website(s), as noted in section a below, which resulted in Defendants gaining unauthorized access to, and unauthorized use of, Dean's mobile device, by Defendants as noted in section b below:

a. m.whitepages.com, a derivative host name of www.whitepages.com, a domain name owned by Defendant WhitePages, Inc., and registered to: WhitePages, Inc., 1301 5th Avenue, Seattle, WA 98101.

b. 

19. Plaintiff Dawn Harbin ("Harbin"), is a citizen and resident of Burleson, Texas, (Burleson County). On information and belief, Harbin incorporates all allegations within this complaint. At all relevant times herein, Harbin owned a mobile device, used that mobile device, on one or more occasions during the class period, in the city of residence, to access the internet sites of one (1) or more Defendant Ringleader Digital Affiliates' website(s), as noted in section a below, which resulted in Defendants gaining unauthorized access to, and unauthorized use of, Harbin's mobile device, by Defendants as noted in section b below:

a. m.whitepages.com, a derivative host name of www.whitepages.com, a domain name owned by Defendant WhitePages, Inc., and registered to: WhitePages, Inc., 1301 5th Avenue, Seattle, WA 98101.

b. 

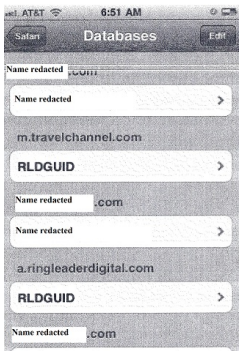
20. Plaintiff Stephanie Owens ("Owens"), is a citizen and resident of Dallas, Texas, (Dallas County). On information and belief, Owens incorporates all allegations within this complaint. At all relevant times herein, Owens owned a mobile device, used that mobile device, on one or more occasions during the class period, in the city of residence, to access the internet sites of one (1) or more Defendant Ringleader Digital Affiliates' website(s), as noted in section a below, which resulted in Defendants gaining unauthorized access to, and unauthorized use of, Owen's mobile device, Defendants as noted in section b below:

a. entertainment.foxnews.mobi, and politics.foxnews.mobi, are derivative host names of www.foxnews.com, a domain name owned by Defendant FOX News Network, LLC, and registered to: Twentieth Century Fox Film Corporation, 10201 W. Pico Boulevard, Los Angeles, CA, 90035; and Foxnews.mobi, a domain name owned by Defendant FOX News Network, LLC, and registered to: Twentieth Century Fox Film Corporation, 10201 W. Pico Boulevard, Los Angeles, CA, 90035.

b. 

21. Plaintiff Ryan Groeneweg ("Groeneweg"), is a citizen and resident of Burleson, Texas, (Burleson County). On information and belief, Groeneweg incorporates all allegations within this complaint. At all relevant times herein, Groeneweg owned a mobile device, used that mobile device, on one or more occasions during the class period, in the city of residence, to access the internet sites of one (1) or more Defendant Ringleader Digital Affiliates' website(s), as noted in section a below, which resulted in Defendants gaining unauthorized access to, and unauthorized use of, Groeneweg's mobile device, by Defendants as noted in section b below:

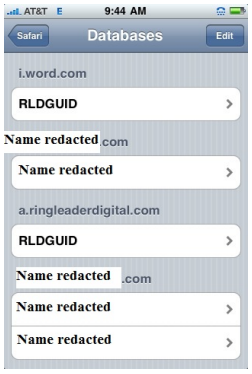
a. m.travelchannel.com, a derivative host name of www.travelchannel.com, a domain name owned by Defendant Travel Channel, LLC, and registered to: The Travel Channel, LLC, 9721 Sherrill Blvd, Knoxville, TN 37932.

b. 

22. Plaintiff Billy Gueringer ("Gueringer"), is a citizen and resident of Waco, Texas, (McLennan County). On information and belief, Gueringer incorporates all allegations within this complaint. At all relevant times herein, Gueringer owned a mobile device, used that mobile

device, on one or more occasions during the class period, in the city of residence, using their mobile device to access the internet sites of one (1) or more Defendant Ringleader Digital Affiliates' website(s), as noted in section a below, which resulted in Defendants gaining unauthorized access to, and unauthorized use of, Gueringer's mobile device, by Defendants as noted in section b below:

a. i.word.com, a derivative host name of www.merriam-webster.com, a domain name owned by Defendant Merriam-Webster, Inc., and registered to: Merriam-Webster Inc., PO BOX 281, Springfield, MA 01102.

b. 

23. Plaintiff Maulik Parikh ("Parikh"), is a citizen and resident of Colleyville, Texas, (Tarrant County). On information and belief, Parikh incorporates all allegations within this complaint. At all relevant times herein, Parikh owned a mobile device, used that mobile device, on one or more occasions during the class period, in the city of residence, to access the internet sites of one (1) or more Defendant Ringleader Digital Affiliates' website(s), as noted in section a below, which resulted in Defendants gaining unauthorized access to, and unauthorized use of, Parikh's mobile device, by Defendants as noted in section b below:

a. cnnmoney.mobi, a domain name owned by Defendant Cable News Network, and registered to: Turner Broadcasting System, Inc., One CNN Center, 13 North, Atlanta, GA 30303.

b. 

24. Plaintiff Richard Weiner ("Weiner"), is a citizen and resident of Dallas, Texas, (Dallas County). On information and belief, Weiner incorporates all allegations within this complaint. At all relevant times herein, Weiner owned a mobile device, used that mobile device, on one or more occasions during the class period, in the city of residence, to access the internet sites of one (1) or more Defendant Ringleader Digital Affiliates' website(s), as noted in section a below, which resulted in Defendants gaining unauthorized access to, and unauthorized use of, Weiner's mobile device, by Defendants as noted in section b below:

a. www.accuweather.com, a domain name owned by Defendant AccuWeather, Inc., and registered to: AccuWeather, Inc., 385 Science, Park Road, State College, PA 16803.

b. 

25. Plaintiff Steve Williams ("Williams"), is a citizen and resident of Dallas, Texas, (Dallas County). On information and belief, Williams incorporates all allegations within this complaint. At all relevant times herein, Williams owned a mobile device, used that mobile

device, on one or more occasions during the class period, in the city of residence, to access the internet sites of one (1) or more Defendant Ringleader Digital Affiliates' website(s), as noted in section a below, which resulted in Defendants gaining unauthorized access to, and unauthorized use of, Williams' mobile device, by Defendants as noted in section b below:

a. m.espn.go.com, a derivative host name of www.espn.com, a domain name owned by Defendant ESPN, Inc., and registered to: ESPN, Inc., 935 Middle Street, Bristol, CT 06010.

b. 

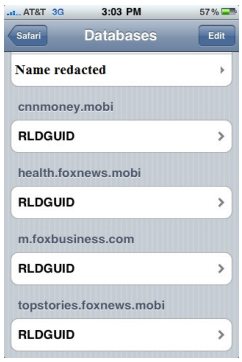
26. Plaintiff G.G. ("Gueringer"), is a citizen and resident of Robinson, Texas, (McLennan County). On information and belief, Gueringer incorporates all allegations within this complaint. At all relevant times herein, Gueringer owned a mobile device, used that mobile device, on one or more occasions during the class period, in the city of residence, to access the internet sites of one (1) or more Defendant Ringleader Digital Affiliates' website(s), as noted in section a below, which resulted in Defendant Ringleader gaining unauthorized access to, and unauthorized use of, Gueringer's mobile device, by Defendants as noted in section b below:

a. m.whitepages.com, a derivative host name of www.whitepages.com, a domain name owned by Defendant WhitePages, Inc., and registered to: WhitePages, Inc., 1301 5th Avenue, Seattle, WA 98101.

b. 

27. Plaintiff Semyon Narosov ("Semyon N."), is a citizen and resident of Dallas, Texas, (Dallas County). On information and belief, Semyon N. incorporates all allegations within this complaint. At all relevant times herein, Semyon N. owned a mobile device, used that mobile device, on one or more occasions during the class period, in the city of residence, to access the internet sites of one (1) or more Defendant Ringleader Digital Affiliates' website(s), as noted in section a below, which resulted in Defendants gaining unauthorized access to, and unauthorized use of, Semyon N.'s mobile device, by Defendants as noted in section b below:

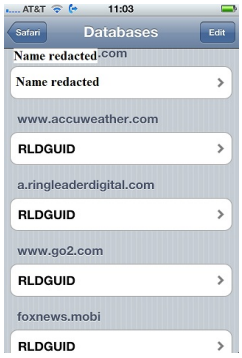
a. cnnmoney.mobi, a domain name owned by Defendant Cable News Network, and registered to: Turner Broadcasting System, Inc., One CNN Center, 13 North, Atlanta, GA 30303; and health.foxnews.mobi, m.foxbusiness.com, topstories.foxnews.mobi, are derivative host names of www.foxnews.com, a domain name owned by Defendant FOX News Network, LLC, and registered to: Twentieth Century Fox Film Corporation, 10201 W. Pico Boulevard, Los Angeles, CA, 90035.

b. 

28. Plaintiff J.N. ("Jenna N."), a minor, age twelve (12) years old, is a citizen and resident of Dallas, Texas, (Dallas County). On information and belief, Jenna N. incorporates all allegations within this complaint. At all relevant times herein, Jenna N. owned a mobile device, used that mobile device, on one or more occasions during the class period, in the city of residence, to access the internet sites of one (1) or more Defendant Ringleader Digital Affiliates' website(s), as noted in section a below, which resulted in Defendants gaining unauthorized access to, and unauthorized use of, Jenna N.'s mobile device, by Defendants as noted in section b below:

a. www.accuweather.com, a domain name owned by Defendant AccuWeather, Inc., and registered to: AccuWeather, Inc., 385 Science, Park Road, State College, PA 16803; foxnews.mobi, a domain name owned by Defendant FOX News Network, LLC, and registered to: Twentieth Century Fox Film Corporation, 10201 W. Pico Boulevard, Los Angeles, CA, 90035; www.go2.com, a domain name owned by Defendant Go2 Media, Inc., and registered to: Go2 Directory Systems, 133 Federal Street, Fifth Floor, Boston, MA 02110; i.word.com, a derivative host name of www.merriam-webster.com, a domain name owned by Defendant Merriam-Webster, Inc., and registered to: Merriam-Webster Inc., PO BOX 281, Springfield, MA 01102; and

m.whitepages.com, a derivative host name of www.whitepages.com, a domain name owned by Defendant WhitePages, Inc., and registered to: WhitePages, Inc., 1301 5th Avenue, Seattle, WA 98101.

b. 

29. Defendant Ringleader Digital, Inc., is a Delaware corporation headquartered in New York, a privately owned corporation, doing business online, using domains which include, but not limited to: Ringleader.com (hereinafter referred to as "Ringleader"), which maintains its headquarters at 286 Fifth Avenue, 6th Floor, New York, NY 10001. Defendant Ringleader Digital, Inc., does business throughout the United States, and in particular, does business in State of New York and in this judicial district.

30. Ringleader's website, http://www.ringleaderdigital.com, (last accessed September 30, 2010) describes its business as follows:

- "Ringleader has focused on being the world's premier ad serving solution provider, delivering the online equipment of ad serving technology and functionality to the mobile and new media markets."

31. Ringleader's "Privacy Policy," dated March 3, 2009, (last accessed September 30, 2010), states in part: "What we collect. Our Media Stamp technology tells us that we have encountered your mobile device at some point (e.g., when you viewed one of our participating web site's ads). We collect non-personally identifiable information from your device, such as

Carrier IP addresses, the request url (the URL that requests the ad which can contain within it information such as your zip code, state, and country, if passed on to us by our publisher partners), as well as http headers from the ad requests coming from participating websites. These headers can contain standard data such as the types of file formats supported by your device, whether or not content can be cached on your device, and the referring URL (i.e. the url of the page you are currently on).

Compelled Disclosure/ Enforcement. We may disclose any information we have to government authorities, and to other third parties when compelled to do so by government authorities or otherwise as required or permitted by law, including but not limited to in response to court orders and subpoenas. We also may disclose information in connection with investigations, for example if we believe in good faith it is necessary in order to investigate, prevent, or take action regarding illegal activities, suspected fraud, situations involving potential threats to the physical safety of any person, violations of our rights or property, or as otherwise required by law."

32. Ringleader's "Privacy Policy," dated March 3, 2009, (last accessed September 30, 2010), as it relates to its use of a Unique Device ID ("UDID") an unknown tracking device, as opposed to cookies, a known tracking device:

> *"The other reason we use it [as opposed to cookies] is because we want to be able to honor consumers' privacy choices persistently,"* Walczak said.

- In regard to "Enhancing the user's experience" by allowing them to use their privacy settings to opt-out of any unauthorized access within their mobile device, such as deleting the RLDGUID targeting, which created a mechanism to "target in perpetuity," is best described by the following:

> *"Maintaining the RLD GUID in the database on a user's device allows us to ensure that the user's opt-out request is being honored."*

Bob Walczak, CEO, Ringleader Digital

33. Ringleader's "Terms of Use," dated March 3, 2009, (last accessed September 30, 2010), as it relates to the "transparency" of the RLDGUID tracking "stamp", is best described by the following:

> *"The stamp is located in [Web site code]," he says. "They would have to take down the mobile Web to get at it."*

http://www.forbes.com/2008/11/06/mobile-cookies-advertising-tech-wire-cx_ew_1106cookies.html

- In regard to a user's ability to use their security settings to delete or "lose" the cookies, is best described by the following:

> *"There is no way to lose the cookie,"* says Walczak. *"Even if you hard reset your phone, the stamp can persistently identify it."*

34. Elizabeth Woyke, "Cookies For Your Cellphone" (last accessed September 28, 2010), online: http://www.forbes.com/2008/11/06/mobile-cookies-advertising-tech-wire-cx_ew_1106cookies.html

35. Defendant AccuWeather, Inc. (hereinafter "AccuWeather"), is a Pennsylvania corporation which maintains its headquarters at 385 Science Park Road, State College, PA 16803. Defendant AccuWeather does business throughout the United States, and in particular, does business in State of New York and in this judicial district.

36. AccuWeather's website, http://www.accuweather.com, describes its business as:

- "We provide local forecasts for everywhere in the United States and over two million locations worldwide. We also provide our products and services to more than 175,000 paying customers in media, business, government and institutions."

37. Defendant AccuWeather has derived online access to any and all previous privacy policies for the period of this Class Action. This Discovery shall be required to compare all

privacy policies within the class period. AccuWeather's "Privacy Policy," dated October 1, 2010 (last accessed October 15, 2010), states in part:

- "Vendors and Third Party Providers. To make the AccuWeather Sites more valuable to our customers and our visitors, we may offer some products, services or features in conjunction with Providers. Many wireless products, for example, may be made available through cooperative arrangements with Providers who offer specialized products, information or services that work well with AccuWeather Sites, products and services. In some instances, our Providers may have the same access to your PII as we do. Their use of the information will be subject to the terms of their respective privacy policies or statements, which you may find on their websites.

  - We use third-party advertising companies to serve ads when you visit the AccuWeather Site(s). These companies may use information about your visits to this and other Web sites in order to provide advertisements about goods and services of interest to you. If you would like more information about this practice and to know your choices about not having this information used by these companies, click here: (http://networkadvertising.org/consumer/opt_out.asp). You may also go to the sites and policies of our Providers to find out more about technologies utilized by them in the course of providing services to the AccuWeather Sites. Some of these Providers are as follows:

    Ringleader Digital and its Media Stamp technology:

    http://ringleaderdigital.com/privacy-policy

    Ringleader Opt-out http://tinyurl.com/RLDOPTOUT

FlashCookies/HTML5 Software/Local Storage/Mini databases. The AccuWeather Sites may utilize flashcookies/HTML5 software and/or local storage and/or mini databases in conjunction with the use of the sites and the targeting of advertising to the users of the AccuWeather sites. Many hand held mobile devices use these technologies in conjunction with the mobile browsers on the devices. Many mobile devices use these technologies which allow for the storage of information on the mobile devices and, in effect, allow the enhancement of internet browsing as well as other uses including but not limited to targeting advertisements. The flashcookies/HTML5/local storage/mini databases technologies also allow the device to track a user's web browsing movements across the internet and not just on one particular website. AccuWeather and its providers may utilize one or more of these technologies and others on the AccuWeather Sites(s)."

38. Defendant's AccuWeather's "most recent" privacy policy still fails to provide adequate information regarding the extent of the Defendants actions, made the basis of this action.

39. Defendant Cable News Network, Inc. (hereinafter "CNN"), is a Delaware corporation which maintains its headquarters at One CNN Center, Atlanta, GA 30303. Defendant CNN does business throughout the United States, and in particular, does business in State of New York and in this judicial district.

40. CNN's website, http://www.cnn.com, describes its business as:

- "CNN.com is among the world's leaders in online news and information delivery."

41. CNN's "Privacy Policy," dated May 20, 2009 (last accessed October 15, 2010), states in part:

- "We may on occasion combine information we collect through our sites with information that we collect from other sources."
- "To enhance your online experience, we use "cookies" or similar technologies. Cookies are text files placed in your computer's browser to store your preferences. Cookies do not contain personally identifiable information; however, once you choose to furnish a site with personally identifiable information, this information may be linked to the data stored in the cookie."
- "We, our third party service providers, advertiser or our partners may also use "web beacons" or clear .gifs, or similar technologies, which are small pieces of code placed on a web page, to monitor the behavior and collect data about the visitors viewing a web page. For example, web beacons may be used to count the users who visit a web page or to deliver a cookie to the browser of a visitor viewing that page."

42. Defendant CNN's Privacy Policy fail to reference its association with Ringleader Digital Inc.

43. Defendant ESPN, Inc. (hereinafter "ESPN"), is a Delaware corporation which maintains its headquarters at 935 Middle St., Bristol, CT 06010. Defendant ESPN does business throughout the United States, and in particular, does business in State of New York and in this judicial district.

44. ESPN's website, http://www.espn.com, its business can be described as: "Entertainment and Sports Programming Network, is an American cable television network dedicated to broadcasting and producing sports-related programming 24 hours a day."

45. ESPN's "Privacy Policy," dated May 6, 2008 (last accessed October 15, 2010), states in part: "does not provide the identity of all associated advertising networks nor all purposes for its involvement."

46. Defendant ESPN's Privacy Policy fail to reference its association with Ringleader Digital Inc.

47. Defendant FOX News Network, LLC (hereinafter "FOX"), is a Delaware corporation which maintains its headquarters at 1211 Avenue of the Americas, New York, NY 10036. Defendant FOX, does business throughout the United States, and in particular, does business in State of New York and in this judicial district.

48. FOX's website, http://www.foxnews.com, its business best described as: "Fox News Channel (FNC), commonly referred to as Fox News or Fox, is a cable and satellite television news channel owned by the Fox Entertainment Group, a subsidiary of News Corporation. As of April 2009, it is available to 102 million households in the United States and further to viewers internationally, broadcasting primarily out of its New York City studios."

49. FOX's "Privacy Policy," dated January 8, 2009 (last accessed October 15, 2010), states in part:

- "We may also obtain PII from third parties."
- "Third party advertisements displayed on FOX's sites may also contain cookies set by Internet advertising companies or advertisers. FOX does not control these advertiser cookies and visitors to our web site(s) should check the privacy policy of the Internet advertising company or advertiser to see whether and how it uses cookies."
- "FOX may use cookies and similar tools to relate your use of our web site(s) to PII obtained from you or a reputable third party. For example, if you've asked us to provide you

information about our upcoming products or promotions, cookie and/or click stream data about your activities on FOX web sites may allow us to limit the materials we provide you to items we think you will find interesting, based on your prior online activities and preferences. However, if FOX wishes to combine your personal and cookie and click stream information in this manner, we will obtain your express affirmative consent."

50. Defendant FOX's Privacy Policy fail to reference its association with Ringleader Digital Inc.

51. Defendant Go2 Media, Inc. (hereinafter "Go2 Media"), is a Delaware corporation which maintains its headquarters at 10 High Street, Tenth Floor, Boston, MA 02110. Defendant Go2 Media, does business throughout the United States, and in particular, does business in State of New York and in this judicial district.

52. Go2 Media's website, http://www.go2.com, describes its business as a: "go2 media connects mobile publishers, local audiences and advertisers through content and location-based advertising.

53. Go2 Media's "Privacy Policy," states in part:

- "go2.com contains links to other sites whose information practices may be different than ours. Visitors should consult the other sites' privacy policies, as we have no control over information that is submitted to or collected by websites that are not our own."
- "In the course of serving advertisements to the go2.com site, our third-party advertising companies may place or recognize a unique "cookie" on your mobile phone's browser."

54. Defendant Go2 Media's Privacy Policy fail to reference its association with Ringleader Digital Inc.

55. Defendant Merriam-Webster, Inc. (hereinafter "Merriam-Webster"), is a Delaware corporation which maintains its headquarters at 47 Federal Street, Springfield, MA 01102. Defendant Merriam-Webster, does business throughout the United States, and in particular, does business in State of New York and in this judicial district.

56. Merriam-Webster's website, http://www.merriam-webster.com, describes its business as: "For more than 150 years, in print and now online, Merriam-Webster has been America's leading and most-trusted provider of language information."

57. Merriam-Webster's "Privacy Policy," dated September 27, 2010 (last accessed October 15, 2010), states in part:

- "Merriam-Webster works with several ad networks that use cookies or beacons to provide you with ads that are relevant to you."
- "Merriam-Webster uses the services of one or more third parties to present or target the advertisements, promotions, and other marketing messages that you may see on various Web pages, to conduct research about such advertisements, promotions, and other marketing messages, and to analyze visits to this and other Web sites. To do this, such third-party providers may collect anonymous data through the use of cookies, beacons, and by other means."

58. Defendant Merriam-Webster's Privacy Policy fail to reference its association with Ringleader Digital Inc.

59. Defendant Travel Channel, LLC (hereinafter "Travel Channel"), is a Delaware corporation which maintains its headquarters at 5425 Wisconsin Avenue, Suite 500, Chevy Chase, MD 20815. Defendant Travel Channel does business throughout the United States, and in particular, does business in State of New York and in this judicial district.

60. Travel Channel's website, http://www.travelchannel.com, describes its business as a: "Travel Channel is available in more than 95 million US cable homes, and its high-definition simulcast, Travel Channel HD™ is distributed to more than 17 million. The website, TravelChannel.com, which serves as the network's entertainment travel hub, averages more than 2 million unique users monthly and its mobile content platform, Travel Channel GO™, is a leading provider of quality mobile travel video and audio content. Travel Channel also manages the leading online travel blog, WorldHum.com."

61. Travel Channel's "Privacy Policy" dated December 10, 2009 (last accessed October 15, 2010), states in part: provides a link regarding opt-out of behavioral tracking to NAI, which does not show the involvement of Ringleader.

62. Defendant Travel Channel's Privacy Policy fail to reference its association with Ringleader Digital Inc.

63. Defendant WhitePages, Inc. (hereinafter "WhitePages"), is a Delaware corporation which maintains its headquarters at 1301 Fifth Ave, Suite 1600, Seattle, WA 98101. Defendant WhitePages does business throughout the United States, and in particular, does business in State of New York and in this judicial district.

64. WhitePages' website, http://www.whitepages.com, describes its business as a: "WhitePages is your go-to source for the most reliable contact information online for the U.S. With one-click access to over 200 million adults and more than 15 million businesses, we make finding and connecting with others incredibly simple—and incredibly free."

65. WhitePages' "Privacy Policy," dated September 20, 2010 (last accessed October 15, 2010), states in part:

- "There are several categories of information that we may collect from you:

- Public Information
- Imported Contacts and Uploaded Files (excluding any Public Information)
- Private Information
- Search Information
- General Information"

66. Defendant WhitePages' Privacy Policy fail to reference its association with Ringleader Digital Inc.

67. Ringleader Terms of Use and Privacy Policy relate only to individuals that access its website by choice and with actual notice, which excludes any method or means involving browser hijacking; thus omitting the Plaintiffs and Class Members.

68. The conduct of Ringleader individually and in concert with the Ringleader Digital Affiliates, individually and jointly, is a fraud that has been perpetrated for years, facilitated, and coordinated, by some of the world's largest websites and the network advertising industry, thereby costing the Class upwards of tens of millions of dollars. Defendant has been systematically defrauding Class Members in a covert operation of surveillance made possible by their gross misconduct, negligence, apparent coordination, and actual fraud, and violating one (1) or more of the following:

a) Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (the "CFAA");

b) Electronic Communications Privacy Act 18 U.S.C. §2510 (the "ECPA"); and

c) Trespass to Personal Property / Chattels

69. Defendant Ringleader and Ringleader Digital Affiliates' privacy documents describe "associations," misleading the users which interpret such to be associated corporate subsidiaries, withholding accurate information that such includes other entities than advertising networks, such as: advertising networks, data exchanges, traffic measurement service providers, marketing and analytic service providers.

70. Defendant Ringleader and Ringleader Digital Affiliates' websites, and its tracking services, are owned by parent companies that have many subsidiaries and fail to provide adequate information about third-party information sharing, different than affiliate sharing, which is subject to more restrictions, including opt-in or opt-out consent requirements. These restrictions are based upon the heightened risk associated with sharing information with unrelated entities, which have different incentives than the entity that collected the user data.

71. Defendant Ringleader and Ringleader Digital Affiliates do not make adequate distinctions between sharing with affiliates, contractors, and third parties, instead, vaguely stating that they do not share user data with unrelated third parties and vaguely disclosing that they share data with affiliates. Users must interpret an affiliate to be a third party, but given the actual usage of these terms of Ringleader Digital Affiliates' privacy policies, that assumption would be mistaken.

72. Defendant Ringleader and Ringleader Digital Affiliate users are unable to identify the corporate families to which these Defendant websites belong; which makes it difficult for a user to discover exactly who such associated entities are, thus their practices are deceptive. A practice is deceptive if it involves a representation, omission or practice that is likely to mislead a consumer acting reasonably in the circumstances, to the consumer's detriment. The conflicting statements in the privacy policies would most likely confuse or mislead a reasonable consumer. The confusion would also likely be to their detriment, as surveys indicate that users do not want companies to collect data about them without permission.

73. Defendant Ringleader and Ringleader Digital Affiliates' privacy documents discuss that the data collection practices of entities associated with their corporations are outside the coverage of their privacy policies. This appears to be an attempt to create a critical loophole

used by Ringleader Digital Affiliates compounding their attempts to violate the privacy protection of their users.

74. Defendant Ringleader and Ringleader Digital Affiliates' privacy documents fail to provide adequate notice that Defendant Ringleader and Ringleader Digital Affiliates allow access to personal behavioral data of their users, including but not limited to, such data embedded with their cookies, to Ringleader, which in turn shares the data with its marketing partners or corporate affiliates and subsidiaries, meaning that user behavior will be profiled by any other entities with whom those sites may choose to share this information. Defendant Ringleader and Ringleader Digital Affiliates state they do not share data with third parties, but they do share data with affiliates, suggesting that they only share data with companies under the same corporate ownership.

75. Defendant Ringleader and Ringleader Digital Affiliates' privacy documents referenced the use of cookies, but state such is used only for audience measurement and not behavioral ad-targeting. The opt-out is inconspicuous on their privacy page and appears in a small font header.

76. Defendant Ringleader and Ringleader Digital Affiliates' privacy documents do not expressly state that if a Ringleader Digital Affiliate user opts-out that behavioral information will not be collected and shared, but only that the Defendant Ringleader and Ringleader Digital Affiliate user will not receive Internet based advertising content from its "advertising delivery service"; moreover its opt-out "unique cookie value" includes identifying information which means the cookie is no longer non-unique.

77. Defendant Ringleader and Ringleader Digital Affiliates' privacy documents falsely imply some level of protection for the user. Defendant Ringleader and Ringleader Digital

Affiliates' privacy documents are sufficiently vague so as to refrain from fully disclosing information to their users about what information is collected through their websites and their associated entities, how the information is used, and the purposes for the collection and use of this information, negating the possibility for their users to provide informed and meaningful consent to these practices. Without adequate notice and informed and meaningful user consent, users had no control over their personal information, thus, the potential privacy dangers were not readily apparent to most users.

78. Defendant Ringleader and Ringleader Digital Affiliates' privacy documents require college-level reading skills for comprehension and include substantial legalese, ambiguous and obfuscated language designed to confuse, disenfranchise, and mislead the users.

79. Defendant Ringleader and Ringleader Digital Affiliates' privacy documents incorporate a multitude of hedging and modality markers so as to minimize their use of covert surveillance technology and data-gathering tools, while sending mixed messages related to privacy controls, advising users that choosing to exercise such controls would cause in whole, or part, diminished functionality of their websites, while such documents emphasize all cookies are very small, thus unobtrusive, and pose no threat since "many websites use them."

80. Defendant Ringleader and Ringleader Digital Affiliates' privacy documents fail to adhere to an adequate notice and choice regime, predicated on user choice, and informed by privacy policies. Defendant Ringleader and Ringleader Digital Affiliates' privacy documents provided nuanced situations that created conditional yes or no answers to these basic questions about a site's data collection and sharing practices, thus it is unclear how an average user could ever understand these practices since the nuances were not explained in the privacy policy. Choice, therefore, cannot be inferred.

81. Defendant Ringleader and Ringleader Digital Affiliates' privacy documents carefully attempt to parse the definitions of phrases related to their tracking activity. Their privacy documents are more nuanced than such categorized analysis allows for, omitting any direct reference to cookies, embedding any and all purposes for its use of surveillance technology into the user's mobile device hardware, use of user's mobile device hardware to store data, use of technology to allow the perpetual mobile device tracking and surveillance of any and all mobile device Internet activity of the Ringleader Digital Affiliate user as evidenced by the attempt to hide its covert activity by referring to their use of "other technologies," or "similar technologies" to cookies and web beacons, in lieu of cookies which would have perpetual existence on a user's mobile device.

82. Defendant Ringleader and Ringleader Digital Affiliates' privacy documents fail to provide notice that their data storage practices as they relate to the period for which user data is stored, have no term period, and are indefinite.

83. Defendant Ringleader and Ringleader Digital Affiliates' privacy documents' verbiage was deceptive by design. This deception is especially troubling when compared with the obligation imposed upon their mobile device visitors to download, read, and comprehend the vast amount of documents required to protect one's mobile device privacy, complicated by the cumulative effect of such task.

84. In addition to downloading, reading and comprehending all of the Ringleader Digital Affiliates websites privacy documents, its users would be required to locate and do the same for the website for the Ringleader, and repeat this obligation. To accentuate the improbability of completing this task though, Ringleader Digital Affiliates website visitors were not provided any information of the identity of Ringleader.

85. Ringleader Digital Affiliates' users' mobile device privacy protection was premised upon imposed requirement to download, read, and comprehend the accumulation of all privacy documents of Ringleader Digital Affiliates, and Ringleader.

86. A millisecond was the time allotted for the Plaintiffs and Class Members opening a Ringleader Digital Affiliates' webpage, before a Ringleader's intentionally, and with knowledge, its actions were unauthorized, accessed Plaintiffs and Class Members mobile device, without their awareness, knowledge or consent to such actions. Such occurred without the benefit of being advised of the association between Defendant Ringleader Affiliates and Defendant Ringleader, provided adequate time to access, read, and comprehend the Terms of Service/Use and Privacy Policy for Ringleader Digital Affiliates' website, and Ringleader. While only the most technical savvy mobile device users were familiar with cookies, a finite amount of individuals even knew about "GUID", let alone could possibly comprehend the technical aspects inherent within the Defendant's privacy documents.

STATEMENT OF FACTS

A. Background

87. This consumer class action involves a pattern of covert mobile device surveillance. The Defendant Ringleader, operated individually and in concert with Ringleader Digital Affiliates to access and use consumers' mobile device and information obtain from users' mobile devices.

88. Defendants did so without such users' authorization.

89. Defendants transmitted a program, information, code, and/or command, to set a Global Unique Identifier ("GUID") within the user's mobile device's database. The GUID

functioned as a unique and persistent identifier use by Defendants to track users' mobile web-browsing activities.

90. In addition, Defendants used the GUID to defeat users' control of their mobile devices, in that Defendants stored the GUID on users' devices in a way that could not reasonably be detected, and so that the GUID could be used to restore Ringleader's persistent tracking ability if a user deleted the Ringleader databases or cookies on a user's device.

91. The objective of this scheme included, but was not limited to, the interception of the mobile devices' properties and the carrier properties and users' web-browsing activities, in order to harvest the consumers personal information from mobile device browsing activities.

B. Mobile Tracking

92. There are basically two approaches to collecting web analytics data. The first, "page tagging," uses a small bit of JavaScript code placed on each web page to notify a third-party server when a page has been viewed by a web browser. Etags can be used in place of cookies. They are a part of caching in HTTP: The server sends the user the tag, and when the user accesses the resource again their web browser sends the tag back. The server uses the tag the browser sent to decide whether to send the user the data or provide data to the browser that the data hasn't changed, and to keep using the old copy.

93. The second and more traditional approach to web analytics is "log file analysis", where the log files that Web servers use to record all server transactions are also used to analyze website traffic.

94. The technological barriers in the area of mobile analytics concern data collection, since not all mobile barriers execute JavaScript so collection of analytic data is not obtained across all devices, and its inability to obtain unique visitor identification. IP addresses on mobile

browser can change as they switch from tower to tower and many mobile devices will take the IP address if the gateway making all the devices look like the same "person."

95. Ringleader placed a globally unique identifier or "GUID," a special type of identifier used in software applications to provide a unique reference number, into mobile devices, Ringleader Digital Inc. accomplished this task.

96. All advertising seeks "state maintenance" or the idea that the person/browser/phone that saw the ad preforms some later activity. Because most phones don't support fully functional browsers, they also don't support the "Cookie:" header, thus not obtaining "uniqueness," necessary to obtain "state maintenance." Obtaining the user's IP address won't work because most mobile phones don't have a public IP address. They access the web through Network Address Translation at the carrier, meaning that many phones are seen by the entire web as all one IP. Some mobile devices though use the x-up-subno header which is not only a unique number to which anything may be linked, and with some carriers, the number itself directly contains most of a phone number. Unlike traditional cookies a user has no choice whatsoever here. A user can't opt-out, since it is always sent. It can't be deleted since it always stays the same. A user cannot use a block cookies tool, as they would in a browser since it is hard coded into a user's phones software. Mobile Advertising benefits from user's lack of knowledge of x-headers and x-up-subno.

97. Mobile Internet advertising currently consists of streaming graphic files, in real time, into content rendered by a user's mobile device browser. Image and text call to action advertising tags are embedded in the content at a publisher's content management system. This occurs prior to delivery of the actual content to the user over the wireless network. Current mobile practice for many of the server side include ad serving systems, so as to log delivery of

user impressions when the ad tags are transmitted from the ad server, across the Internet to the publisher's content system, whether or not they actually arrive.

98. Mobile advertising systems also lacks reliable browser cookies while traditional online advertising relies on the use browser cookies, implementations inherent in conventional implementations of mobile ad serving have effectively prevented mobile advertising from being effective. Moreover, the deficiencies inherent in all known mobile advertising techniques have, to a significant extent, collectively inhibited the use of mobile advertising in general.

99. Mobile phone devices are nearly always specific to one user, whiile computers may have multiple users. Parents desiring their children to possess mobile devices for security are not aware their children are being "commercially stalked." The fact that mobile phone devices provide access to real time context of location, presence, and device capabilities, combined with multiple communication capabilities of voice, SMS, email and browsing allows exploitation of all parties, including minors, by mobile advertisers. The result is that minor children are using mobile devices and unknown parties know their location, in addition to the ultimate details of their lives. Class representative Semyon Narosov noting his concerns, reproduced literatim without [sic], regarding his minor children, including J.N.J.N., a minor, aged twelve (12) years of age, being "commercially stalked" in general, but not case specific:

> *"To whom it may concern:*
> *I'm a single parent of 4 girls. ages 10, 12, 14, and 16, I purchased four I-phones for them, When I checked one of them and saw what was happening, I was very unsettled. The mere thought of the possibility gets me into very unhappy state. WHO ARE THESE PEOPLE? WHY DO THEY HAVE MY DAUGHTER'S LOCATION, THREE OF THEM ARE TEENAGERS AND ONE IS ONLY 10! WHAT ARE THOSE PEOPLE DOING WITH THE INFORMATION? What is the parent supposed to do, This is outrageous. When information of 10 year old is shared because she wanted to play a game or went to website that appeared interesting? Where is the information stored? Who buys it? What do the do with it? where and when my child travels to? This is a clear violation of the personal*

and private information that should be protected. When did that became a norm sell the information where the 10 or 12 years old girl having a slumber party?

C. Ringleader Digital Inc.'s Technology

100. Ringleader describes its business practices as:

> *"Ringleader Digital brings the online advertising experience to mobile√ëfulfilling the potential and promise of the mobile Web. Ringleader's device-agnostic network is the only third-party mobile ad service, and is the first to specifically target ads by device functionality. Ringleader simplifies advertising transactions and delivery by providing brands and publishers the ability to seamlessly and simultaneously distribute ad campaigns across any mobile digital platform. With this unprecedented control, publishers maximize the revenue potential for ad campaigns while brands and advertisers can finally track and audit every element of a campaign's effectiveness."*

"Ringleader Digital Redefines Mobile Advertising with Groundbreaking Tracking of Individual User Activity Across the Mobile Ecosystem" (last accessed September 30, 2010), online: http://ringleaderdigital.com/ringleader-digital-redefines-mobile-advertising-with-groundbreaking-tracking-of-individual-user-activity-across-the-mobile-ecosystem

101. Ringleader Digital business practices may be better analyzed by a review of a patent application which includes Ringleader Digital's CEO Robert Walczak and provides details noted within the patent's abstract, and a schematic diagram relating to a "Device Identification Request," which is the same or similar technology used by Defendant Ringleader Digital Inc., made the basis of this action. This application claims the benefit of U.S. Provisional Patent Application Ser. No. 61/091,816, filed Aug. 26, 2008, entitled, "MOBILE COOKIE ARCHITECTURE." Such patent also includes the following entry in the transaction history:

USPTO application number 12/548,080, petition decision- dismissed, 9-30-2010.

(19) **United States**

(12) **Patent Application Publication**

Landsman et al.

(10) **Pub. No.: US 2010/0057843 A1**

(43) **Pub. Date: Mar. 4, 2010**

(54) **USER-TRANSPARENT SYSTEM FOR UNIQUELY IDENTIFYING NETWORK-DISTRIBUTED DEVICES WITHOUT EXPLICITLY PROVIDED DEVICE OR USER IDENTIFYING INFORMATION**

(76) Inventors: **Rick Landsman**, Cortland Manor, NY (US); **Robert J. Walczak, JR.**, New York, NY (US)

Correspondence Address:
WELSH & FLAXMAN LLC
2000 DUKE STREET, SUITE 100
ALEXANDRIA, VA 22314 (US)

(21) Appl. No.: **12/548,080**

(22) Filed: **Aug. 26, 2009**

Related U.S. Application Data

(60) Provisional application No. 61/091,816, filed on Aug. 26, 2008.

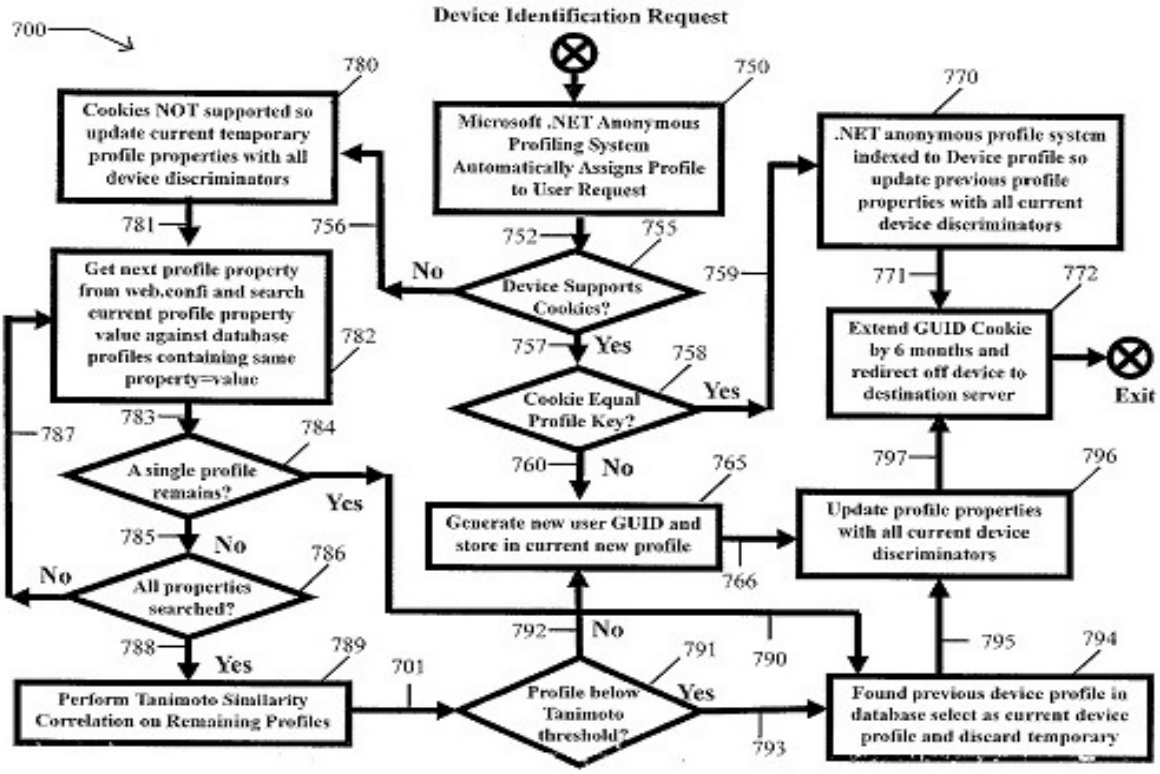
Publication Classification

(51) **Int. Cl.**
G06F 15/16 (2006.01)
G06F 17/30 (2006.01)

(52) **U.S. Cl.** **709/203**; 709/224; 707/104.1; 707/10; 707/3; 707/E17.108; 707/E17.044

(57) **ABSTRACT**

A technique for uniquely identifying devices without explicitly provided device or user identifying information in a networked client-server environment, e.g., the Mobile Internet, in which content is downloaded from a server to a device browser executing at a client device, and using static XML markup tags embedded in the content in a manner transparent to a user situated at the device browser, derives a globally unique device identifier. Device identifying information is captured and maintained in a device profile database associated with a globally unique device identifier. Specifically, mark up code embedded into a referring content page effectively downloads software from a distribution server, and then instantiates the software in the client device browser. The software transparently and dynamically inserts an Internet address request to a device identification management system. The device identification management system selects a device profile associated with a previously detected request from the device and retrieves its globally unique identifier from a database of all profiles for all previous devices requesting unique device identifications. If a matching profile is not found in the database, the device identifying information associated with the request is entered as a new device profile along with a globally unique identifier associated with that specific device in the database. The globally unique identifier is delivered back to the device or external systems for their own use, e.g., mobile Internet advertising management systems.



D. NO- "Path 756"- Unauthorized Access

102. Plaintiffs and Class Members purchased specific mobile devices for a multitude of reasons which include the benefits of its privacy and security protections, as exemplified by the iPhone, and its operating system:

> *"Safe and secure by design. iOS 4 is highly secure from the moment you turn on your iPhone. All apps run in a safe environment, so a website or app can't access data from other apps. iOS 4 supports encrypted network communication to protect your sensitive information. Optional parental controls let you manage iTunes purchases, Internet browsing, and access to explicit material. To guard your privacy, apps requesting location information must get your permission first. You can set a passcode lock to prevent unauthorized access to your phone and configure iPhone to delete all your data after too many unsuccessful passcode attempts. And in the event your iPhone is lost or stolen, a MobileMe membership allows you to find your iPhone on a map and remotely delete all data.3 If you get it back, you can restore everything from your last backup."*

Apple iPhone, "The world's most advanced mobile operating system," (last accessed October 15, 2010), online: http://www.apple.com/iphone/ios4/

103. The iPhone provides a global control that allows a user to control location tracking, set by default in the off position. In regard to cookies, this mobile device includes a default setting that cookies will only be accepted by websites "visited." This would negate the settings of cookies set by "non-visited" sites, such as Defendant Ringleader, a "third party" advertising network, which was not visited by Plaintiffs and Class Members, iPhone users are also provided the ability to clean history, cookies and cache. The benefits of the privacy and security protection provided by the iPhone represents a common benefit for mobile devices, and used by Plaintiffs and Class Members.

104. Defendant Ringleader knew that mobile devices would block third party cookies by default, and Plaintiffs and Class Members who attempted to block cookies, relied on such privacy and security protections. Defendant Ringleader implemented a plan, using its technology, to bypass properties within the mobile device of the Plaintiffs and Class Members, ignoring their privacy and security choices, with the intent to have unauthorized access to, and unauthorized use of the Plaintiffs and Class Members mobile devices, and exemplified by "No-Path 756," as opposed to "Yes- Path 757."

105. Defendants unauthorized access to the Plaintiffs and Class Members mobile device is evidenced, in whole or part, by either its use of the "No-Path 756" and "Yes-Path 757," noted within the section referenced: "Device Identification Request," Patent Application 20100057843. "Yes- Path 757" relates to the path followed if the user's device accepts cookies while "No-Path 756" relates to the path followed if cookies are not allowed by the mobile device.

106. Plaintiffs and Class Members that allowed cookies from first party websites, but not third party entities like Defendant Ringleader, and cleared their mobile devices of cookies,

history, and cache, had their privacy and security choices thwarted by Defendants who re-spawned the tracking data:

- "[0122] This is a special unique device identification cookie value and is initialized to zero the first time set before verifying the end device supports cookies. If cookies are supported this value will be set with the "NAME" property above as a way to distinguish first time visitors from previous visitors already in the database. It should be appreciated that although cookies are implemented in accordance with the present invention, the present invention allows for unique identification of client devices in all cases, regardless of whether or not cookies are supported by the client device. Not all client device support cookies, e.g., less than 50% devices support cookies from our analysis of past campaigns. From a scalability and performance perspective, for those client devices that do support cookies there is no database search required rather the cookie becomes the direct index to the device profile, so if the present system is capable of setting and reading a cookie in the client device, it behooves us to take advantage of that fact, but for those that don't we have other discriminators we use to search the database for a previous profile for the device. If someone clears their cookies we can still identify the device using all the other discriminators."

107. Defendants' unauthorized access to the Plaintiffs and Class Members' mobile devices was accomplished knowingly and intentional, best evidenced by reviewing the insidious navigation involved in "No-Path 756." Defendant's actions were not inadvertent, nor could they be construed to be accidental:

- "[0111] Decision block 755, as previously described, tests whether the mobile device browser 7 as shown in FIG. 1A, supports the setting and transmission of cookies to a server. In this scenario, as signified by the NO path 756, either the client device 5 does not

support or has been configured not to allow persisting server browser cookies. Alternatively, the carrier's Internet gateway may filter out device browser cookies to prevent them from being set or passed to the Internet server. In which case, block 780 is invoked; signifying cookies cannot be set or read by the Unique Device Identification Management System 400."

E. Unauthorized Scan

108. Many Internet users are familiar with rogue anti-spyware applications that pop-up on their screen after visiting a website only to automatically start a scan of your hardware, listing a myriad of spyware infections within your computer, and offering the sale of an anti-spyware tool to clean your hardware. Defendant's scan is not transparent.

109. Plaintiffs and Class Members did not authorize Defendants to perform a scan of their mobile devices. Defendants actions were intentional, not inadvertent, with knowledge that Plaintiffs and Class Members did not expressly consent to a scan of their mobile devices:

- "[0064]The script executing at the mobile device browser, 7 in the client device 5, reads from inside the client device 5 additional unique device identification information, such as the client device, clock and time zone settings, any unique device detection cookie values previously set in the client device 5 accessible by the script, as well as information for the version number of the mobile device browser 7 itself, to name a representative sample. These values are appended to the unique device identification management system request Internet URL address as keyword=value parameters. The script then dynamically inserts the direct unique device identification request tags into the HTML code in content page 35, as symbolized by block 58. Generally speaking, the mobile device browser 7 in response to executing the dynamically inserted unique device identification request tags, issues a request for device

identification, as symbolized by line 60, to the Unique Device Identification Management System 400, connected through communication link 23 to Internet 10b."

110. Defendant Ringleader's "RLD Device Detector" accomplishes the unauthorized scan of Plaintiffs and Class Members mobile devices:

"RLD Real Time. Access to immediate, actionable data is what many mobile, online and analytics platforms have been missing. Now, thanks to RLD Real Time™, powered by RLD Media Stamp™, RLD Device Detector™ and RLD Context Extractor™, publishers, agencies and analytics companies can plug into a rich body of data to mobilize their services in real time — at a cost that is solely based on usage. Over 140 pieces of data can be captured by Real Time™ such as the device attributes, its location, the applications it runs, what ad sizes and formats can be displayed, and its carrier information. Media Stamp™ can also identify, map and track which actions have or haven't been taken in response to ads by unique users in real time throughout multiple sessions. The RLD Context Extractor™ provides rich context profiles, producing a taxonomy to target advertising campaigns against."

Ringleader Digital, "RLD Real Time™," (last accessed October 15, 2010), online: http://ringleaderdigital.com/our-solutions/rld-real-time.

111. Defendants objectives included, but was not limited to, obtaining a mobile device "Fingerprint," a practice of obtaining device information to perpetually identify the mobile device as "indirect identification," which can be linked to additional data elements to identify "personable identifiable information" ("PII"), personal information and/ or sensitive information.

112. The collection of data by Defendants was wholesale and all-encompassing. Data passing through the users' mobile devices was acquired by Defendants without discrimination as to the kind, type, nature, or sensitivity of the data. Regardless of any representations to the

contrary—all data—whether sensitive, financial, personal, private, complete with all identifying information, was intercepted.

F. Unauthorized Creation of Databases

113. Plaintiffs and Class Members did not authorize Defendants to create databases within their mobile devices. The databases used by Defendants did not exist prior to Plaintiffs and Class Members visiting the Ringleader Digital Affiliates websites.

114. The use of Local Storage on mobile devices and emergence of advertisers using local storage in combination with a Global Unique Identifier ("GUID's") was cited within the W3C draft pertaining to "web storage." "W3C," a non-profit World Wide Web consortium whose mission revolves around the development and standardization of web technologies. In an attempt to standardize client-side storage, the Web Hypertext Application Technology Working Group (WHATWG) came up with a well-structured client-side storage solution, which is part of the HTML5 specifications approved by W3C; however such provided a "manifesto" for some in the mobile industry:

> *"A third-party advertiser (or any entity capable of getting content distributed to multiple sites) could use a unique identifier stored in its local storage area to track a user across multiple sessions, building a profile of the user's interests to allow for highly targeted advertising. In conjunction with a site that is aware of the user's real identity (for example an e-commerce site that requires authenticated credentials), this could allow oppressive groups to target individuals with greater accuracy than in a world with purely anonymous Web usage.*
>
> *There are a number of techniques that can be used to mitigate the risk of user tracking:*
>
> ***Treating persistent storage as cookies***
> *If users attempt to protect their privacy by clearing cookies without also clearing data stored in the local storage area, sites can defeat those attempts by using the two features as redundant backup for each other. User agents should present the interfaces for clearing these in a way that helps users to understand this*

> *possibility and enables them to delete data in all persistent storage features simultaneously. [COOKIES]"*

W3C Editor's Draft, "Web Storage" (last accessed September 30, 2010), online: http://dev.w3.org/html5/webstorage/

115. In concept, HTML5 Local Storage is very similar to cookies. On a per origin basis, there is a set of disk-persisted name/value pairs within the client web browser. Like cookies, this data persists even after the user navigates away from the web site, close their browser tab, or exit their browser, like cookies, this data can be transmitted to the remote web server. Unlike all previous attempts at providing persistent local storage, it is implemented natively in web browsers, so it is available even when third-party browser plugins are not.

116. HTML5 appeals to the mobile advertising industry as a substitute for traditional cookies that do not function well on mobile devices. Like flash cookies, HTML5 cookies are not stored in a browser "cookies" file, and again, like flash cookies, can be used to track users across websites, but also have privacy implications. A study released by researchers at the University of New York, Berkeley and other universities, submitted to the federal government for consideration as part of a new policy on the use of tracking technologies, revealed the details of online privacy invasion of epidemic proportions, that reverberated globally.

> *"Of the top 100 websites, 31 had at least one overlap between a HTTP and Flash cookie. For instance, a website might have an HTTP cookie labeled "uid" with a long value such as 4a7082eb-775d6-d440f-dbf25. There were 41 such matches on these 31 sites. Most Flash cookies with matching values were served by third-party advertising networks. That is, upon a visit to a top 100 website, a third party advertising network would set both a third party HTTP cookie and a third party Flash cookie."*

Ashkan Soltani, Shannon Canty, Quentin Mayo, Lauren Thomas, Chris Jay Hoofnagle, "Flash Cookies and Privacy" (10 August 2009), online: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1446862.

117. Plaintiffs and Class Members were unable to access the Defendants database located within their own mobile device, but could view the amount of storage used and available.

While tracking cookies are normally 4 KB, and Defendants claimed it stored only a tracking cookie in the Plaintiffs and Class Members mobile device database, and tracking cookies should be identical size to all Plaintiffs and Class Members, there were varying mobile device storage limits used:

1) Class Representative Andrew Hillman: 19.6 KB

2) Class Representative Semyon Narosov: 12.6 KB

3) Class Representative Dr. Richard Weiner: 8.0 KB

118. Databases may be used, and tables created, within a database only after direct connection is made to the database. The Defendant knowingly and without authorization created the databases, made the basis of this action. When a database is opened, an empty database is automatically created if the database requested does not exist. Thus, the processes for opening and creating a database are identical.

G. Media Stamp

119. Ringleader Digital's "media stamp" technology, made the basis of this action, is basically using some of the modern HTML5 capabilities of mobile browsers to perform the same tasks as a traditional cookie, but out of sight of most users. Media Stamp, is not technically a mobile cookie since it's not browser based, is on the server side, thus it cannot be affected by anti-cookie technologies employed by carriers such as gateway stripping (a technique that renders the cookies useless or unreliable for ad targeting), and preventing users from deleting them.

120. Wireless carriers typically prevent outside firms from embedding such information in mobile devices. "The carriers strip off third-party cookies," says Bob Walczak, chief executive of Ringleader Digital. To get around the carriers, Ringleader Digital embeds its

digital stamp in servers rather than browsers, although mobile devices forbid the use of third party software in Applications to collect and send Device Data to a third party for processing or analysis, banning "Third Party" Analytics.

121. In a non-technical version, what Ringleader does do is have certain advertising properties, such as AccuWeather include a small JavaScript on their mobile site. An invisible iFrame is created which loads code from the RLD website. This website determines if they've seen you before and setup the right RLDGUID database (for the RLD domain) and then communicates through iFrame message-passing to its parent (the AccuWeather website) that it should create a mirror of this database for the Accuweather.com domain.

122. Once a user visits a RLD enabled mobile site a copy of the exact same data for each site that uses their tracking shall be duplicated. This is so that it's easier to re-spawn if one or the others get damaged or deleted, but it also means that any script running on the Ringleader Digital Affiliates, such as the AccuWeather domain, could grab your GUID.

123. The Web SQL Database spec is not involved since browsers won't implement it, and the specification is dormant. All of the browsers support Local Storage. Each website creates a local host entry that points back to the RLD tracker such as rld.accuweather.com. That's in the AccuWeather domain so blocking the RLD domain won't limit this surveillance activity.

124. Software scripts get inserted through ad requests embedded in publisher content that then execute inside or outside the device on a time sliced basis. The software scripts delivered, execute in content pages for very limited time periods. Upon completion of the time slice, the script is replaced with the actual requests for device identification services to an anonymous unique device identification management system.

125. The stamp or cookie, placed on Ringleader Digital Affiliates, captures user data by tracking up to 100 "discriminators," such as a user's time zone, mobile browser and mobile Web bookmarks. After weighing these factors, the stamp assigns each user a unique digital descriptor. Because the technology lives on site servers, it will work on nearly all Web-enabled phones, regardless of carrier. On information and belief, Plaintiffs and Class Members that used their mobile devices and visited Ringleader Digital Affiliates sites had Defendants perform the unauthorized tasks as noted within the United States Patent Application, 20100057843:

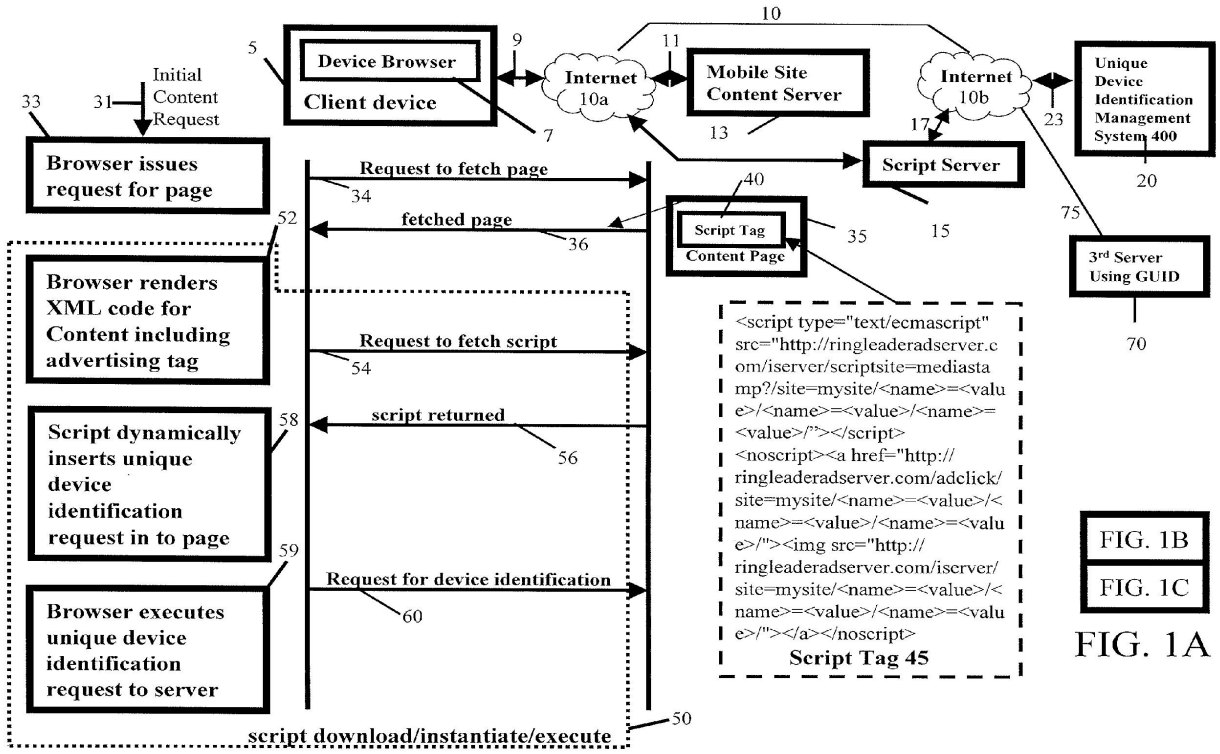


FIG. 1B

FIG. 1C

FIG. 1A

126. Subsequent content page navigation by the user, whether within a session or during subsequent sessions, can be obtained directly from the local content cache. No additional load over the network is required. If the cache is cleared, the process merely repeats to refresh the scripts the next time a unique device identification management system request tag is rendered.

127. Plaintiffs and Class Members who became aware of Defendants tracking device embedded within their mobile device storage attempted various methods of deleting. The database of both Defendants Ringleader and Defendant Ringleader Digital Affiliates only to have the databases re-spawn within their mobile device.

H. Opt Out? When did I opt in!

128. Mobile phones are used for everything from banking and investing to shopping and communicating with others through email or chat programs. Although online communications may not be considered "top secret," mobile users do not want third parties reading their email, or examining personal information stored on their mobile devices (such as financial statements), or downloading tracking software, such as setting a Global Unique Identifier ("GUID") within their mobile device database, without their knowledge or consent.

129. Browser cookie controls and preference settings provide greater user privacy control. The purpose of a browser privacy mode is to allow users to browse the Internet without leaving data tracks. Browsers save visited websites in the browsing history, downloaded files in the download history, search terms in the search history, and data typed into online registration forms including cached version of such files. Cookie controls allow the user to decide which cookies can be stored on their mobile devices and transmitted to websites, and using parental controls to block specific content by adjusting the tabs located within the user's browser. Defendants business practices relied on the fact that Safari users could not turn off their databases for the iPhone, iPod touch, or iPad, nor could users view the low-level details about the data within their browsers, browser history, cookies, and cache that is currently stored; moreover Safari's mobile web browser do not include privacy features such as no "private

browsing," which would have the ability to block or clear individual application cookies or access to local browser cache.

130. Safari is set by default to block all third-party cookies. If a user has not changed those settings, this option effectively accomplishes the same thing as setting the opt-out cookie, thus Defendant(s) use of the users database provided a "safe haven," since users incorrectly interpreted their browser settings provided privacy and security protections.

131. Cookie controls and user privacy preference settings provide user protection, but the Defendant Ringleader responded with new technology to override user's preferences on their own mobile devices, and set identical code in the Plaintiffs and Class Members' mobile devices resulting in a uniform action to set redundant unique identifiers used to identify and track users.

132. Ringleader Digital's privacy page says that users can opt-out "for life" from the company's tracking if they direct their mobile device's Web browser to http://tinyurl.com/RLDOPTOUT; however Ringleader Digital Affiliate users were never provided any information of its association with Ringleader.

133. Ringleader's opt-out mechanism was also flawed by those users that miraculously could have figured out the association between Ringleader Digital Affiliates and Ringleader and located the Ringleader opt-out page: "the opt-out will be effective for the life of the device unless you install a new browser, or update your existing browser, in which case you will need to re-implement the opt-out utility in order to maintain your opt-out status." Users desiring that Defendant Ringleader be denied any and all tracking of their mobile devices in any regard were denied such option, in that, even if a user opted-out of Ringleader they would still be tracked but not be sent targeted ads, thus provided no consideration for the user's preferences.

134. Ringleader Digital's opt-out system provides no way for a user to confirm that their ID stored in the Safari database has been opted-out from tracking, including a recent revision, and Ringleader Digital essentially says that the database must remain on the device if you want to remain opted-out. Since deleting the database will mean that the servers can't identify the opted-out user as the same device that they're not supposed to track.

135. Users trying to get rid of the database deleted the RLDGUID databases, cleared cookies, and then went to the opt-out link, it did indeed eliminate the unique identifier that had been tracking; however, it did not stop Ringleader Digital's partner sites from recreating the cookies and Safari databases with a new persistent RLDGUID.

136. "If you clear cookies or clear the database, it's not opting-out," Walczak said. "If you opt-out with just the link, it will change the ID to an opt-out ID. On the back-end we set a token on our system that says this ID is opted-out and we won't send targeted advertising to that device." Ringleader claims that there are no best-practice guidelines for this type of technology in the mobile space, but it also asserts that it does provide clear opt-out instructions. "There are no guidelines on this in mobile, but Ringleader is a co-chair of the [Mobile Marketing Association's] standards committee and [we are] on the privacy committee to help to create them," said Bob Walczak, CEO of Ringleader, New York.

137. Individuals have a reasonable expectation of privacy in their personal mobile phone, the integrity of their mobile phone, and the confidentiality of their communications with the Internet websites that they visit, using their Internet connection to transmit and receive personal and private data, including but not limited to, personal emails, personal Internet research and viewing, credit card information, banking information, personal identifiable information such as social security number, date of birth, and medical information.

I. Defendants' Harmful Business Practices

138. At all relevant times, Defendants' advertising technology has contained secret information-gathering capacities that were not disclosed to or known by Plaintiffs or the Class and which permitted Defendants to surreptitiously, in an unauthorized manner, and for tortious and unlawful purposes, intercept and access Plaintiffs' and the Class Members' personal and private information, monitor their Internet activity, and create detailed personal profiles based on such information.

139. At all relevant times, Plaintiffs and the Class, as part of their normal Internet browsing and usage, visited websites that unbeknownst to them utilized and/or facilitated tracking and profiling technology. Since they were doing so in the privacy of their own homes or offices, and since Defendants did not display any warning or indication that they were collecting or transmitting personal and private information to or from their computer systems, Plaintiffs and the Class had a reasonable expectation of privacy as to the nature of their activity and the contents of any information they provided to or obtained from a particular website.

140. Defendants have used surreptitious data-collection methods to secretly intercept and access mobile device users' personal data and web browsing habits and have transmitted this information to Defendants for its own commercial benefit.

141. Defendants collected and/or disclosed covered information of Class Members about their online activity, including across websites.

142. Defendants' business practice unfairly wrests control from users who choose to delete any mobile device database and their cookies in order to avoid being tracked. Users who are aware of this may delete their databases and cookies periodically, believing that the new cookies and databases they receive will contain new unique identifiers, thus hindering the ability

of advertising networks to track their behavior across sites. Using databases to re-identify users overrides this control, with little available redress for users. Although users may arguably protect themselves by periodically deleting their cookies and databases as well, the means for doing so are extremely obscure and difficult even for savvy consumers to use.

143. Defendants failed to disclose that its applied technologies also provide Defendants with the ability to surreptitiously intercept, access, and collect electronic communications and information from unsuspecting Internet users—including Plaintiffs and the Class.

144. Defendants intercepted Class Members' electronic communications for the purpose of committing a tortious or criminal act, and violated the constitutional rights of Plaintiffs and Class Members.

145. In all cases where some notice was provided, that notice was insufficient, misleading, and inadequate. Consent under such circumstances was impossible.

146. In no case as alleged in this complaint, was adequate, informed notice provided to any Class Members of the true nature and function of the Defendants service.

147. Defendants failed to provide opt-out functionality. Defendants' opt-out process required the user to leave the user's mobile device, link to a webpage that was not disclosed within the confines of the RLD affiliates privacy document, to set their security preferences.

148. In any case where the opportunity of 'opting out' of the Defendants service was provided, such 'opt-out' rights were misleading, untrue, and deceptive.

149. In no case was the collection of all Internet communication data between the consumer and the Internet halted or affected in any way. All data was still collected. The 'opt-out' only affected what advertisements the consumer was shown. Thus, the provision of the opportunity for opting-out was, itself, totally misleading.

150. Plaintiffs and the Class Members did not voluntarily disclose their personal and private information prior to the user opting-out of the Defendant's tracking, let alone, after the user opted-out, including their Internet surfing habits, to Defendants - and indeed never even knew that Defendants existed or conducted data collection and monitoring activities upon and across its Plaintiffs and Class Members' websites. Plaintiffs and the Class Members provided such information, and had their Internet habits monitored, without their knowledge or consent, and would not have consented having their personal and private information, including their on-line profiles, used for Defendants' commercial gain.

151. Defendants did not obtain consent from Plaintiffs and Class Members for any collection or use and was not allowed to decline consent at the time such statement was presented to the Class Members.

152. Defendants did not obtain consent from Plaintiffs and Class Members for any disclosure of covered information to unaffiliated parties and was not allowed to decline consent at the time such statement was presented to the Class Members.

153. Defendants intentionally accessed Plaintiffs and Class Members' mobile devices without authorization or exceeded authorized access to obtain information from a protected mobile devices, involved an interstate communications.

154. Defendants sold, shared, and/or otherwise disclosed covered information of Class Members to an unaffiliated party without first obtaining the consent of the Class Members to whom the covered information related to.

155. At all relevant times, Plaintiffs and Class Members' personal and private information was intercepted by and/or accessed by Defendants and transmitted to it on a regular basis, without alerting Internet users in any manner. As a result, Defendants were able to and did

access Plaintiffs' and Class Members' mobile devices and/or intercept their electronic communications without authorization. Defendants have obtained, compiled, and used this personal information for its own commercial purposes.

156. Defendants intercepted Class Members' electronic communications for the purposes of implanting unauthorized cookies and databases on Class Members' mobile devices; repeatedly accessing electronic communications without Class Members' knowledge and consent so as to profile such persons' web browsing habits, secretly tracking Class Members' activities on the Internet and collecting personal information about consumers; and profiting from the use of the illegally obtained information, all to Defendants' benefit and Class Members' detriment.

157. Defendants intentionally intercepted, endeavored to intercept, or procured another person to intercept or endeavor to intercept the electronic communication of Plaintiffs and Class Members.

158. Defendants have knowingly, recklessly, or negligently disclosed, exploited, misappropriated and/or engaged in widespread commercial usage of Plaintiffs' and the Class' private and sensitive information for Defendants' own benefit without Plaintiffs' or the Class' knowledge, authorization, or consent. Such conduct constitutes a highly offensive and dangerous invasion of Plaintiffs' and the Class' privacy.

159. Defendants used and consumed the resources of the Plaintiffs and Class Members' mobile devices and substantially increased their Internet bandwidth by gathering user information and transferring such to Defendants.

160. Defendants caused harm and damages to Plaintiffs and Class Members' mobile devices finite resources, depleted and exhausted its memory, thus causing an actual inability to

use it for its intended purposes, and significant unwanted CPU activity, usage, and network traffic, resulting in instability issues.

161. Defendants caused harm and damages to the Plaintiffs and Class Members including but not limited to, consumption of their device's finite resources, memory depletion which resulted in the actual inability to use if for its intended purposes.

162. Defendants' downloads were not evident. Users assumed that the issues relate to hardware, Windows installation problems, or viruses, and resorted to contacting technical support experts, or even buying a new mobile device because the existing system mobile device posed privacy risks.

163. Class Members attempting to repair their own mobile device risked damaging their system files. Badly infected systems required a clean reinstallation of all their software in order to return to full functionality, with charges of a few hundred dollars to remove viruses and spyware, and unauthorized cookies, if serviced in house, or on site such costs exceeded $40-$60 per hour.

164. Defendants harmed Plaintiffs and Class Members by its actions which included, but not limited to the following:

a) Loss of valuable data by attempts to remove cookies and databases once discovered;

b) Incurred economic losses accompanied by an interruption in service;

c) Functionality of mobile device was interfered with, including an inability of websites visited once content was disabled;

d) Information was deleted, otherwise made unavailable;

e) Impaired the integrity and availability of data, programs and information.

165. Defendant Ringleader's activities with Ringleader Digital Affiliates occurred throughout the United States, and have secretly obtained personal and private information from Plaintiffs and the Class - a course of action and a body of information that is protected from interception, access, and disclosure by federal law.

166. Defendants used, interfered with, and intermeddled with Class Members' ownership of their personal property, namely, their mobile devices, by, directly or indirectly, secretly depositing cookies and databases on their mobile devices, secretly accessing their mobile devices to obtain information contained in and enabled by the Global Unique Identifier, and secretly collecting personal data and information regarding each Class Members' Internet surfing habits contained in electronic storage on his/her mobile device.

167. Defendants Ringleader and Ringleader Digital Affiliates failed to disclose that its software, tracks and stores information regarding consumers' Internet use and other forms of advertisements on consumers' mobile devices based on such use. The installation of such tracking device would be material to consumers in their decision whether to install the software offered by Defendants. Defendants Ringleader and Ringleader Digital Affiliates furthered their deceitful practices by storing the tracking files in locations on consumers' mobile device that is rarely accessed by consumers.

168. Defendants Ringleader and Ringleader Digital Affiliates' technology wrongfully monitored Internet users' activities at each and every website users visited and the wrongfulness of this conduct is multiplied by the fact that Defendants aggregate this information about users' habits across numerous websites and unjustly enriched Defendants to the severe detriment of Plaintiffs and the Class. Plaintiffs and the Class have been harmed, as they have been subjected to repeated and unauthorized invasions of their privacy - violations which continue to this day.

169. The vast majority of Internet users will continue to be tracked by dozens of companies — companies they've never heard of, companies they have no relationship with, companies they would never choose to trust with their most private thoughts and reading habits.

CLASS ALLEGATIONS
Allegations as to Class Certification

170. Pursuant to Federal Rule of Civil Procedure 23(a), (b)(1), (b)(2), and (b)(3), Plaintiffs bring this action as a Class action, on behalf of themselves and all others similarly situated as members of the following Classes (collectively, the "Class"):

a) U.S. Resident Class: All persons residing in the United States that accessed a Ringleader Digital Affiliate website and Defendant set a Global Unique Identifier ("GUID") within the user's mobile device's database to back the mobile device's Identifier for purposes of restoring it later if deleted by the user.

b) U.S. Minors Resident Class: All persons residing in the United States, are all below the age of thirteen (13) years of age and all U.S. Minors Resident Class are also members of the U.S. Resident class.

c) Injunctive Class: All persons after the date of the filing of this complaint, residing in the United States, that accessed a Ringleader Digital Affiliate website and Defendant set a Global Unique Identifier ("GUID") within the user's mobile device's database to back the mobile devices Identifier for purposes of restoring it later if deleted by the user.

171. The Class action period, (the "Class Period"), pertains to the date, two years preceding the date of this filing to the date of Class certification.

172. Plaintiffs reserve the right to revise this definition of the Class based on facts learned in the course of litigation of this matter.

173. On behalf of the U.S. Resident and New York Resident Classes, Plaintiffs seek equitable relief, damages and injunctive relief pursuant to:

a) Computer Fraud and Abuse Act, 18 U.S.C. § 1030;

b) Electronic Communications Privacy Act 18 U.S.C. § 2510; and

c) Trespass to Personal Property / Chattels

174. On behalf of the Injunctive Class, Plaintiffs seek only injunctive relief.

175. **Persons Excluded From Classes:** Subject to additional information obtained through further investigation and discovery, the foregoing definition of the Class may be expanded or narrowed by amendment or amended complaint. Specifically excluded from the proposed Class are Defendant, their officers, directors, agents, trustees, parents, children, corporations, trusts, representatives, employees, principals, servants, partners, joint venturers, or entities controlled by Defendant, and their heirs, successors, assigns, or other persons or entities related to or affiliated with Defendant and/or their officers and/or directors, or any of them; the Judge assigned to this action, and any member of the Judge's immediate family.

176. Plaintiffs reserve the right to revise these Class definitions of the Classes based on facts they learn during discovery.

177. **Numerosity:** The members of the Class are so numerous that their individual joinder is impracticable. Plaintiffs are informed and believe, and on that basis allege, that the proposed Class contains tens of thousands of members. The precise number of Class Members is unknown to Plaintiffs. The true number of Class Members is known by Defendant, however and, thus, Class Members may be notified of the pendency of this action by first Class mail, electronic mail, and by published notice. Upon information and belief, Class Members can be identified by the electronic records of Defendant.

178. **Class Commonality:** Pursuant to Federal Rules of Civil Procedure, Rule 23(a)(2) and Rule *23(b)(3)*, are satisfied because there are questions of law and fact common to Plaintiffs and the Class, which common questions predominate over any individual questions

affecting only individual members, the common questions of law and factual questions include, but are not limited to:

a) What was the extent of Defendant Ringleader and Ringleader Digital Affiliates' business practice of setting a Global Unique Identifier ("GUID") within the user's mobile device's database to back the mobile devices Identifier for purposes of restoring it later if deleted by the user and how did it work?

b) What information did Defendant Ringleader and Ringleader Digital Affiliates' collect from its business practices of setting a Global Unique Identifier ("GUID") within the user's mobile device's database to back the mobile devices Identifier for purposes of restoring it later if deleted by the user, and what did it do with that information?

c) Whether Ringleader Digital Affiliate users, by virtue of their visitation to Ringleader Digital Affiliate's website, had pre-consented to the operation of Ringleader and Ringleader Digital Affiliates' business practices of setting a Global Unique Identifier ("GUID") within the user's mobile device's database to back the mobile devices Identifier for purposes of restoring it later if deleted by the user;

d) Was there adequate notice, or *any* notice, of the operation of Defendant Ringleader and Ringleader Digital Affiliates' business practices of setting a Global Unique Identifier ("GUID") within the user's mobile device's database to back the mobile devices Identifier for purposes of restoring it later if deleted by the user provided to Defendant Ringleader and Ringleader Digital Affiliates' users?

e) Was there reasonable opportunity to decline the operation of Defendant Ringleader and Ringleader Digital Affiliates' business practices of setting a Global Unique Identifier ("GUID") within the user's mobile device's database to back the mobile devices Identifier for purposes of restoring it later if deleted by the user provided to Defendant Ringleader and Ringleader Digital Affiliates' users?

f) Did Defendant Ringleader and Ringleader Digital Affiliates' business practices of setting a Global Unique Identifier ("GUID") within the user's mobile device's database to back the mobile devices Identifier for purposes of restoring it later if deleted by the user disclose, intercept, and transmit personally identifying information, or sensitive identifying information, or personal information?

g) Whether Defendant Ringleader and Ringleader Digital Affiliates devised and deployed a scheme or artifice to defraud or conceal from Plaintiffs and the Class Defendant Ringleader and Ringleader Digital Affiliates' ability to, and

practice of, intercepting, accessing, and manipulating, for its own benefit, personal information, and tracking data from Plaintiffs' and the Class' personal mobile device via the ability to; (and practice of) implanting secret "cookies" on their mobile device;

h) Whether Defendant Ringleader and Ringleader Digital Affiliates engaged in deceptive acts and practices in, connection with its undisclosed and systemic practice of implanting, accessing and/or disclosing unique identifiers, tracking data, and personal information on Plaintiffs and the Class' personal mobile device and using that data to track and profile Plaintiffs' and the Class' Internet activities and personal habits, proclivities, tendencies, and preferences for Defendant's use and benefit;

i) Did the implementation of Defendant Ringleader and Ringleader Digital Affiliates' business practices of setting a Global Unique Identifier ("GUID") within the user's mobile device's database to back the mobile devices Identifier for purposes of restoring it later if deleted by the user violate the Computer Fraud and Abuse Act, 18 U.S.C. §§ 1030?

j) Did the implementation of Defendant Ringleader and Ringleader Digital Affiliates' business practices of setting a Global Unique Identifier ("GUID") within the user's mobile device's database to back the mobile devices Identifier for purposes of restoring it later if deleted by the user violate the Electronic Communications Privacy Act, 18 U.S.C. § 2510?

k) Did the operation, function, and/or implementation of Defendant Ringleader and Ringleader Digital Affiliates' business practices of setting a Global Unique Identifier ("GUID") within the user's mobile device's database to back the mobile devices Identifier for purposes of restoring it later if deleted by the user cause Trespass to Personal Property / Chattels?

l) Are the Defendant Ringleader and/or Ringleader Digital Affiliates liable under a theory of unjust enrichment for violations of the statutes listed herein?

m) Whether Defendant Ringleader and Ringleader Digital Affiliates participated in and/or committed or is responsible for violation of law(s) complained of herein;

n) Are Class Members entitled to damages as a result of the implementation of Defendant Ringleader and Ringleader Digital Affiliates' marketing scheme, and, if so, what is the measure of those damages?

o) Whether Plaintiffs and members of the Class have sustained damages as a result of Defendant's conduct, and, if so, what is the appropriate measure of damages;

p) Whether Plaintiffs and members of the Class are entitled to declaratory and/or injunctive relief to enjoin the unlawful conduct alleged herein; and

q) Whether Plaintiffs and members of the Class are entitled to punitive damages, and, if so, in what amount.

179. **Typicality:** Plaintiffs' claims are typical of the claims of the members of the Class in that Plaintiffs and each member of the Class accessed a Ringleader Digital Affiliate website and a cookie was set on their mobile device to use the storage within the mobile device database to back up browser cookies for the purposes of restoring them later.

180. **Adequacy of Representation:** Plaintiffs will fairly and adequately protect the interests of the members of the Class. Plaintiffs have retained counsel highly experienced in complex consumer Class action litigation, and Plaintiffs intend to prosecute this action vigorously. Plaintiffs have no adverse or antagonistic interests to those of the Class.

181. **Superiority:** A Class action is superior to all other available means for the fair and efficient adjudication of this controversy. The damages or other financial detriment suffered by individual Class Members is relatively small compared to the burden and expense that would be entailed by individual litigation of their claims against the Defendant. It would thus be virtually impossible for the Class, on an individual basis, to obtain effective redress for the wrongs done to them. Furthermore, even if Class Members could afford such individualized litigation, the court system could not. Individualized litigation would create the danger of inconsistent or contradictory judgments arising from the same set of facts. Individualized litigation would also increase the delay and expense to all parties and the court system from the issues raised by this action. By contrast, the Class action device provides the benefits of adjudication of these issues in a single proceeding, economies of scale, and comprehensive supervision by a single court, and presents no unusual management difficulties under the circumstances here.

182. In the alternative, the Class may be also certified because:

a) the prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudication with respect to individual Class Members that would establish incompatible standards of conduct for the Defendant;

b) the prosecution of separate actions by individual Class Members would create a risk of adjudications with respect to them that would, as a practical matter, be dispositive of the interests of other Class Members not parties to the adjudications, or substantially impair or impede their ability to protect their interests; and/or

c) Defendant have acted or refused to act on grounds generally applicable to the Class thereby making appropriate final declaratory and/or injunctive relief with respect to the members of the Class as a whole.

183. The claims asserted herein are applicable to all persons throughout the United States that accessed a Ringleader Digital Affiliate website and a cookie was set on their mobile device to use the storage within the mobile device database to back up browser cookies for the purposes of restoring them later.

184. The claims asserted herein are based on Federal law and New York law, which is applicable to all Class Members throughout the United States.

185. Adequate notice can be given to Class Members directly using information maintained in Defendant's records or through notice by publication.

186. Damages may be calculated from the information maintained in Defendant's records, so that the cost of administering a recovery for the Class can be minimized. The amount of damages is known with precision from Defendant's records.

Count I
Violation of the Computer Fraud and Abuse Act
18 U.S.C. § 1030 *et seq.*

187. Plaintiffs incorporate the above allegations by reference as if set forth herein at length.

188. Plaintiffs assert this claim against each and every Defendant named herein in this complaint on behalf of themselves and the Class.

189. The Computer Fraud and Abuse Act, 18 U.S.C. § 1030, referred to as "CFAA," regulates fraud and relates activity in connection with computers, and makes it unlawful to intentionally access a computer used for interstate commerce or communication, without authorization or by exceeding authorized access to such a computer, thereby obtaining information from such a protected computer, within the meaning of U.S.C. § 1030(a)(2)(C).

190. Defendant violated 18 U.S.C. § 1030 by intentionally accessing a Plaintiffs' computer, without authorization or by exceeding access, thereby obtaining information from such a protected computer.

191. The Computer Fraud and Abuse Act, 18 U.S.C. § 1030(g), provides a civil cause of action to "any person who suffers damage or loss by reason of a violation" of CFAA.

192. The Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a)(5)(A)(i), makes it unlawful to "knowingly cause[s] the transmission of a program, information, code, or command and as a result of such conduct, intentionally cause[s] damage without authorization, to a protected computer," of a loss to one or more persons during any one-year period aggregating at least $5,000 in value.

193. Plaintiffs' computer is a "protected computer...which is used in interstate commerce and/or communication" within the meaning of 18 U.S.C. § 1030(e)(2)(B).

194. Defendant violated 18 U.S.C. § 1030(a)(2)(C) by intentionally accessing a Plaintiffs' computer, without authorization or by exceeding access, thereby obtaining information from such a protected computer.

195. Defendant violated 18 U.S.C. § 1030(a)(5)(A)(i) by knowingly causing the transmission of a command embedded within their webpages, downloaded to Plaintiffs' computer, which are protected computers as defined in 18 U.S.C. § 1030(e)(2)(B). By accessing, collecting, and transmitting Plaintiffs' viewing habits, Defendant intentionally caused damage without authorization to those Plaintiffs' computers by impairing the integrity of the computer.

196. Defendant violated 18 U.S.C. § 1030(a)(5)(A)(ii) by intentionally accessing Plaintiffs and Class Members' protected computers without authorization, and as a result of such conduct, recklessly caused damage to Plaintiffs and Class Members' computers by impairing the integrity of data and/or system and/or information.

197. Defendant violated 18 U.S.C. § 1030(a)(5)(A)(iii) by intentionally accessing Plaintiffs and Class Members' protected computers without authorization, and as a result of such conduct, caused damage and loss to Plaintiffs and Class Members.

198. Plaintiffs have suffered damage by reason of these violations, as defined in 18 U.S.C. § 1030(e)(8), by the "impairment to the integrity or availability of data, a program, a system or information."

199. Plaintiffs have suffered loss by reason of these violations, as defined in 18 U.S.C. § 1030(e)(11), by the "reasonable cost ... including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service."

200. Plaintiffs have suffered loss by reason of these violations, including, without limitation, violation of the right of privacy, disclosure of personal identifying information,

sensitive identifying information, and personal information, interception, and transactional information that otherwise is private, confidential, and not of public record.

201. As a result of these takings, Defendant's conduct has caused a loss to one or more persons during any one-year period aggregating at least $5,000 in value in real economic damages.

202. Plaintiffs and Class Members have additionally suffered loss by reason of these violations, including, without limitation, violation of the right of privacy.

203. Defendant's unlawful access to Plaintiffs' computers and electronic communications has caused Plaintiffs irreparable injury. Unless restrained and enjoined, Defendant will continue to commit such acts. Plaintiffs' remedy at law is not adequate to compensate it for these inflicted and threatened injuries, entitling Plaintiffs to remedies including injunctive relief as provided by 18 U.S.C. § 1030(g).

Count II
Violations of the Electronic Communications Privacy Act
18 U.S.C. §2510

204. Plaintiffs incorporate the above allegations by reference as if set forth herein at length.

205. Plaintiffs assert this claim against each and every Defendant named herein in this complaint on behalf of themselves and the Class.

206. The Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2510, referred to as "ECPA," regulates wire and electronic communications interception and interception of oral communications, and makes it unlawful for a person to "willfully intercept [], endeavor [] to intercept, or procure [] any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication," within the meaning of 18 U.S.C. § 2511(1).

207. Defendants violated 18 U.S.C. § 2511 by intentionally acquiring and/or intercepting, by device or otherwise, Plaintiffs' and Class Members' electronic communications, without knowledge, consent, or authorization.

208. The contents of data transmissions from and to Plaintiffs' and Class Members' personal computers constitute "electronic communications" within the meaning of 18 U.S.C. §2510.

209. Plaintiffs are "person[s] whose … electronic communication is intercepted … or intentionally used in violation of this chapter" within the meaning of 18 U.S.C. § 2520.

210. Defendants violated 18 U.S.C. § 2511(1)(a) by intentionally intercepting, endeavoring to intercept, or procuring any other person to intercept or endeavor to intercept Plaintiffs' electronic communications.

211. Defendants violated 18 U.S.C. § 2511(1)(c) by intentionally disclosing, or endeavoring to disclose, to any other person the contents of Plaintiffs' electronic communications, knowing or having reason to know that the information was obtained through the interception of Plaintiffs' electronic communications.

212. Defendants violated 18 U.S.C. § 2511(1)(d) by intentionally using, or endeavoring to use, the contents of Plaintiffs' electronic communications, knowing or having reason to know that the information was obtained through the interception of Plaintiffs' electronic communications.

213. Defendants' intentional interception of these electronic communications without Plaintiffs' or Class Members' knowledge, consent, or authorization was undertaken without a facially valid court order or certification.

214. Defendants intentionally used such electronic communications, with knowledge, or having reason to know, that the electronic communications were obtained through interception, for an unlawful purpose.

215. Defendants unlawfully accessed and used, and voluntarily disclosed, the contents of the intercepted communications to enhance their profitability and revenue through advertising. This disclosure was not necessary for the operation of Defendants' system or to protect Defendants' rights or property.

216. The Electronic Communications Privacy Act of 1986, 18 USC §2520(a) provides a civil cause of action to "any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used" in violation of the ECPA.

217. Defendants are liable directly and/or vicariously for this cause of action. Plaintiffs therefore seek remedy as provided for by 18 U.S.C. §2520, including such preliminary and other equitable or declaratory relief as may be appropriate, damages consistent with subsection (c) of that section to be proven at trial, punitive damages to be proven at trial, and a reasonable attorney's fee and other litigation costs reasonably incurred.

218. Plaintiffs and Class Members have additionally suffered loss by reason of these violations, including, without limitation, violation of the right of privacy.

219. Plaintiffs and the Class, pursuant to 18 U.S.C. §2520, are entitled to preliminary, equitable, and declaratory relief, in addition to statutory damages of the greater of $10,000 or $100 a day for each day of violation, actual and punitive damages, reasonable attorneys' fees, and Defendants' profits obtained from the above-described violations. Unless restrained and enjoined, Defendants will continue to commit such acts. Plaintiffs' remedy at law is not adequate

to compensate it for these inflicted and threatened injuries, entitling Plaintiffs to remedies including injunctive relief as provided by 18 U.S.C. § 2510.

Count III
Violations of Section 349 of New York General Busines Law:
Deceptive Acts and Practices

220. Plaintiffs incorporate the foregoing allegations by reference.

221. Defendants' actions alleged herein constitute unlawful, unfair, deceptive and fraudulent business practices.

222. Defendants' conduct constitutes acts, uses and/or employment by Defendants and/or their agents or employees of deception, fraud, unconscionable and unfair commercial practices, false pretenses, false promises, misrepresentations, and/or the knowing concealment, suppression, and/or omission of material facts with the intent that others rely upon such concealment, suppression, or omission, in connection with the sale or advertisement of services, and with the subsequent performance of services and transactions, in violation of section 349 of New York's General Business Law.

223. Defendants' acts and omissions were generally directed at the consuming public, including accountholders.

224. The unfair and deceptive trade acts and practices of Defendants have directly, foreseeably, directly and proximately caused damages and injury to Plaintiffs and the other members of the Class.

225. Defendants' violations of section 349 of New York's General Business Law have damaged Plaintiffs and the other Class members, and threaten additional injury if the violations continue.

226. Defendants' acts and omissions, including Defendants' misrepresentations, have caused harm to Class members in that Class members have suffered the loss of privacy through the exposure of the personal and private information and evasion of privacy controls on their devices.

227. Plaintiffs and the other members of the Class have no adequate remedy at law.

228. Plaintiffs, on his own behalf and on behalf of the Class members, seeks damages, injunctive relief, including an order enjoining Defendants' § 349 violations alleged herein, and court costs and attorneys' fees, pursuant to NY CLS Gen Bus § 349.

Count IV
Trespass to Personal Property / Chattels

229. Plaintiffs incorporate by reference and reallege all paragraphs previously alleged herein.

230. The common law prohibits the intentional intermeddling with personal property, including a mobile device, in possession of another that results in the deprivation of the use of the personal property or impairment of the condition, quality, or usefulness of the personal property.

231. By engaging in the acts alleged in this complaint without the authorization or consent of Plaintiffs and Class Members, Defendant dispossessed Plaintiffs and Class Members from use and/or access to their mobile devices, or parts of them. Further, these acts impaired the use, value, and quality of Plaintiffs' and Class Members' mobile device. Defendant's acts constituted an intentional interference with the use and enjoyment of the computers. By the acts described above, Defendants, has repeatedly and persistently engaged in trespass to personal property in violation of the common law.

232. Without Plaintiffs' and Class Members' consent, or in excess of any consent given, Defendant knowingly and intentionally accessed Plaintiffs' and Class Members' property, thereby intermeddling with Plaintiffs' and Class Members' right to possession of the property and causing injury to Plaintiffs and the members of the Class.

233. Defendant engaged in deception and concealment in order to gain access to Plaintiffs and Class Members' mobile devices.

234. Defendant undertook the following actions with respect to Plaintiffs' and Class Members' computer:

a) Defendant accessed and obtained control over the user's mobile device;

b) Defendant caused the installation of a new code onto the hard drive of the user's mobile device;

c) Defendant programmed the operation of its code to function and operate without notice or consent on the part of the owner of the mobile device, and outside of the control of the owner of the mobile device.

235. All these acts described above were acts in excess of any authority any user granted when he or she visited the Ringleader Digital Affiliates' websites and none of these acts was in furtherance of users viewing the Ringleader Digital Affiliates websites. By engaging in deception and misrepresentation, whatever authority or permission Plaintiffs and Class Members may have granted to Ringleader Digital Affiliates was vitiated.

236. Defendant's installation and operation of its program used, interfered, and/or intermeddled with Plaintiffs' and Class Members' mobile devices. Such use, interference and/or intermeddling was without Class Members' consent or, in the alternative, in excess of Plaintiffs' and Class Members' consent.

237. Defendant's installation and operation of its program constitutes trespass, nuisance, and an interference with Class Members' chattels, to wit, their mobile devices.

238. Defendant's installation and operation of its program impaired the condition and value of Class Members' mobile devices.

239. Defendant's trespass to chattels, nuisance, and interference caused real and substantial damage to Plaintiffs and Class Members.

240. As a direct and proximate result of Defendant's trespass to chattels, nuisance, interference, unauthorized access of and intermeddling with Plaintiffs' and Class Members' property, Defendant has injured and impaired in the condition and value of Class Members' computers, as follows:

a) By consuming the resources of and/or degrading the performance of Plaintiffs' and Class Members' computers (including space, memory, processing cycles, and Internet connectivity);

b) By diminishing the use of, value, speed, capacity, and/or capabilities of Plaintiffs' and Class Members' mobile devices;

c) By devaluing, interfering with, and/or diminishing Plaintiffs' and Class Members' possessory interest in their mobile devices;

d) By altering and controlling the functioning of Plaintiffs' and Class Members' mobile devices;

e) By infringing on Plaintiffs' and Class Members' right to exclude others from their mobile devices;

f) By infringing on Plaintiffs' and Class Members' right to determine, as owners of their mobile devices, which programs should be installed and operating on their mobile devices;

g) By compromising the integrity, security, and ownership of Class Members' mobile devices; and

h) By forcing Plaintiffs and Class Members' to expend money, time, and resources in order to remove the program installed on their mobile devices without notice or consent.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and all others similarly situated, prays for judgment against Defendant as follows:

A. Certify this case as a Class action on behalf of the Classes defined above, appoint Plaintiffs as Class representatives, and appoint their counsel as Class counsel;

B. Declare that the actions of Defendant, as set out above, violate the following:

a) Computer Fraud and Abuse Act, 18 U.S.C. § 1030;

b) Electronic Communications Privacy Act 18 U.S.C. §2510; and

c) Trespass to Personal Property / Chattels

C. As applicable to the Classes *mutatis mutandis*, awarding injunctive and equitable relief including, *inter alia*: (i) prohibiting Defendant from engaging in the acts alleged above; (ii) requiring Defendant to disgorge all of its ill-gotten gains to Plaintiffs and the other Class Members, or to whomever the Court deems appropriate; (iii) requiring Defendant to delete all data surreptitiously or otherwise collected through the acts alleged above; (iv) requiring Defendant to provide Plaintiffs and the other Class Members a means to easily and permanently decline any participation in any data collection activities; (v) awarding Plaintiffs and Class Members full restitution of all benefits wrongfully acquired by Defendant by means of the wrongful conduct alleged herein; and (vi) ordering an accounting and constructive trust imposed on the data, funds, or other assets obtained by unlawful means as alleged above, to avoid dissipation, fraudulent transfers, and/or concealment of such assets by Defendant;

D. Award damages, including statutory damages where applicable, to Plaintiffs and Class Members in an amount to be determined at trial;

E. Award restitution against Defendant for all money to which Plaintiffs and the Classes are entitled in equity;

F. Restrain Defendant, their officers, agents, servants, employees, and attorneys, and those in active concert or participation with them from continued access, collection, and transmission of Plaintiffs and Class Members' personal information via preliminary and permanent injunction;

G. Award Plaintiffs and the Classes:

a) their reasonable litigation expenses and attorneys' fees;

b) pre- and post-judgment interest, to the extent allowable;

c) restitution, disgorgement and/or other equitable relief as the Court deems proper;

d) compensatory damages sustained by Plaintiffs and all others similarly situated as a result of Defendant's unlawful acts and conduct;

e) statutory damages, including punitive damages;

f) permanent injunction prohibiting Defendant from engaging in the conduct and practices complained of herein;

H. For such other and further relief as this Court may deem just and proper.

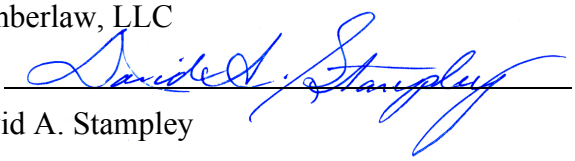
JURY TRIAL DEMAND

The Plaintiffs hereby demand a trial by jury of all issues so triable.

Respectfully submitted,

Dated: November 3, 2010

Kamberlaw, LLC

By: 

David A. Stampley

One of the attorneys for Plaintiffs, individually and on behalf of a class of similarly situated individuals

Scott Kamber (sk5794)
skamber@kamberlaw.com
KamberLaw, LLC
100 Wall Street 23rd floor
New York, New York 10005
Telephone: (212)920-3072
Facsimile: (212) 920-3081

David Stampley (ds0775)
dstampley@kamberlaw.com
KamberLaw, LLC
100 Wall Street 23rd floor
New York, New York 10005
Telephone: (212)920-3072
Facsimile (212) 920-3081

Joseph H. Malley (not admitted)
malleylaw@gmail.com
Law Office of Joseph H. Malley
1045 North Zang Blvd
Dallas, TX 75208
Telephone: (214) 943-6100